AY 2019-2020

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Dental Hygiene HIPAA Policies and Procedures
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions and Concepts of HIPAA Related Terms</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>11</td>
</tr>
<tr>
<td>History</td>
<td>11</td>
</tr>
<tr>
<td>Purpose of the Law</td>
<td>11</td>
</tr>
<tr>
<td>Compliance Dates</td>
<td>12</td>
</tr>
<tr>
<td>State Law</td>
<td>12</td>
</tr>
<tr>
<td>Enforcement</td>
<td>12</td>
</tr>
<tr>
<td>Penalties</td>
<td>12</td>
</tr>
<tr>
<td>FSU Dental Hygiene Policy Statement</td>
<td>15</td>
</tr>
<tr>
<td>Privacy Officer</td>
<td>16</td>
</tr>
<tr>
<td>Privacy Policies and Procedures Statement</td>
<td>17</td>
</tr>
<tr>
<td>Notice of Privacy Practices or NPP</td>
<td>18</td>
</tr>
<tr>
<td>Designated Record Sets</td>
<td>20</td>
</tr>
<tr>
<td>Minimum Necessary</td>
<td>21</td>
</tr>
<tr>
<td>Verification of Identity</td>
<td>23</td>
</tr>
<tr>
<td>Required Disclosures (Whistleblowers &amp; Crime Victims)</td>
<td>25</td>
</tr>
<tr>
<td>Permitted Uses and Disclosures &amp; Decision Tree</td>
<td>27</td>
</tr>
<tr>
<td>Patient Authorization Forms</td>
<td>28</td>
</tr>
<tr>
<td>Subsidized Marketing Communications</td>
<td>30</td>
</tr>
<tr>
<td>Sale of Patient Information</td>
<td>32</td>
</tr>
<tr>
<td>Mitigates Harm</td>
<td>33</td>
</tr>
<tr>
<td>Business Associates</td>
<td>34</td>
</tr>
<tr>
<td>Patient Rights and Requests</td>
<td>35</td>
</tr>
<tr>
<td>Amendment</td>
<td>37</td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>39</td>
</tr>
<tr>
<td>Confidential Communications</td>
<td>41</td>
</tr>
<tr>
<td>Restricted Disclosure</td>
<td>42</td>
</tr>
<tr>
<td>Training</td>
<td>44</td>
</tr>
<tr>
<td>Disciplinary Action (Sanctions) (Whistleblowers &amp; Crime Victims)</td>
<td>45</td>
</tr>
<tr>
<td>Retaliation and Intimidation</td>
<td>47</td>
</tr>
<tr>
<td>Waiver of HIPAA Rights</td>
<td>49</td>
</tr>
<tr>
<td>Documentation of HIPAA Compliance</td>
<td>50</td>
</tr>
<tr>
<td>Safeguard Patient Information</td>
<td>52</td>
</tr>
<tr>
<td>Administrative</td>
<td>52</td>
</tr>
<tr>
<td>Physical</td>
<td>55</td>
</tr>
<tr>
<td>Technical</td>
<td>57</td>
</tr>
<tr>
<td>De-Identification</td>
<td>60</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>62</td>
</tr>
<tr>
<td>Complaints</td>
<td>64</td>
</tr>
<tr>
<td>Fundraising</td>
<td>65</td>
</tr>
<tr>
<td>Review and Revise</td>
<td>66</td>
</tr>
<tr>
<td>Acknowledgement of Receipt of HIPAA Policies and Procedures</td>
<td>67</td>
</tr>
<tr>
<td>APPENDIX (ATTACHMENTS AND FORMS)</td>
<td>68</td>
</tr>
</tbody>
</table>
DEFINITIONS AND CONCEPTS OF HIPAA RELATED TERMS
(Terms are Listed Alphabetically and Underlined)

Throughout this document, the following terms are used:

**Academic Dental Hygiene Practice (a.k.a., Dental Practice)** – reference to the “academic dental hygiene practice” is meant to describe the dental hygiene clinical practice on campus that is a HIPAA covered entity and serves as a learning environment for our dental hygiene students. Dental practice may also be used in lieu of academic dental hygiene practice, with the intention of the description being one and the same.

**Business Associate** – Generally means an entity, or a person who is not a member of the dental practice’s workforce, that performs a service for the dental practice involving patient information. Examples of business associates include a billing service, collection agency, accounting or law firm; consultant, health information organization, e-prescribing gateway, data transmission company that requires access to patient information on a routine basis; and a company that offers patients personal health records on behalf of the dental practice. A dental practice must have a business associate agreement in place with each of the dental practice’s business associates. A business associate subcontractor that has access to patient information is treated as a downstream business associate. A business associate must have a business associate agreement in place with each of the business associate’s subcontractors.

A health care provider, such as a dental laboratory, does not become a business associate when a dental practice discloses patient information to the health care provider for treatment purposes. However, a health care provider may be a business associate of a dental practice if the health care provider performs a service for the dental practice rather than providing treatment for a patient. For example, a dental practice would need a business associate agreement with a health care provider that accesses the dental practice’s patient information for purposes of providing training to the dental practice’s workforce. 45 CFR § 160.103.

**Covered Entity** – A covered entity means:

1. A health plan  
2. A health care clearinghouse  
3. A healthcare provider (such as a dental practice) that transmits any health information in electronic form in connection with a transaction covered by HIPAA 45 CFR § 160.103

**Data Set** – Means a semantically meaningful unit of information exchanged between two parties to a transaction 45 CFR § 162.103.

**De-identified** – In general, patient information is “de-identified” if 18 identifiers are removed, and the remaining information cannot be used alone or in combination with other information to identify the patient. HIPAA does not apply to properly de-identified information.
The 18 identifiers are: names, street address other than town, city, state, and zip code, telephone numbers, fax numbers, email addresses, social security numbers, medical records numbers, vehicle identifiers and serial numbers, including license plates, device identifiers and serial numbers, full face photographs or comparable images, URL’s, IP address numbers, Biometric identifiers (includes finger and voice prints).

**Designated Record Set or Record** – Means any item, collection, or grouping of information that includes patient information and is maintained, collected, used or disseminated by or for the dental practice. Several of patient rights under HIPAA apply only to patient information in a “designated record set”.

Example, a patient has a right to:

- See information about the patient that the dental practice maintains in a designated record set, and/or get copies of information about the patient that the dental practice maintains in a designated record set
- Have the dental practice amend, when appropriate, information or a record about the patient in a designated record set

**HIPAA** – When reference is made to “HIPAA”, it is an abbreviation for HIPAA Privacy, Security and Breach Notification Rules and stands for Health Insurance Portability and Accountability Act.

**Limited Data Set** – A limited data set is a limited set of identifiable patient information as defined in the Privacy Regulations issued under the Health Insurance Portability and Accountability Act. This limited data set of information may be disclosed to an outside party without a patient’s authorization if certain conditions are met. First, the purpose of the disclosure may only be for research, public health, or health care operations. Second, the person receiving the information must sign a data use agreement with Ferris State University. This agreement has specific requirements which are discussed as follows.

A limited data set is information from which specific “identifiers” have been removed. Specifically, as it relates to the individual or his or her relatives, employers, or household members, all of the following identifiers must be removed in order for health information to be in a state of limited data set. Those identifiers are:

- Names
- Street addresses (other than town, city, state, and zip code)
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical records numbers (chart numbers)
- Health plan beneficiary numbers
- Account numbers
- Certificate license numbers
- Vehicle identifiers and serial numbers, including license plates
- Device identifiers and serial numbers
- Full face photographs or comparable images
- URL’s
The health information that may remain in the information disclosed includes:

- Dates such as DOB or DOD, appointment dates (however, see note below)
- City, state, five digit or more zip code
- Ages in years, months or days or hours

It is important to know that this information is still protected health information or PHI under HIPAA. It is not de-identified information and is still subject to the requirements of the Privacy Regulations.

**Data Use Agreements**

Because a limited data set is still PHI, the Privacy Regulations contemplate that the privacy of individuals will be protected by requiring covered entities (Ferris State University) to enter into data use agreements with recipients of limited data sets. The data use agreement must meet standards specified in the Privacy Regulations. A data agreement must:

- Establish the permitted uses and disclosures of the limited data set
- Identify who may use or receive the information
- Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law
- Require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement
- Require the recipient to report to the covered entity any unauthorized use or disclosure of which it becomes aware
- Require the recipient to ensure that any agents (including subcontractors) to whom it provides the information will agree to the same restrictions as provided in the agreement
- Prohibit the recipient from identifying the information or contacting the individuals

The limited data set provisions also require covered entities to take reasonable steps to cure any breach by a recipient of the data use agreement. That is, if Ferris State University determines that data provided to a recipient is being used in a manner not permitted by the agreement, it must work with the recipient to correct this problem. If these steps are unsuccessful, Ferris State University would have to discontinue disclosure of PHI to the recipient under the data use agreement and report the problem to the Department of Health and Human Services (HHS.gov).

**(Creating the Limited Data Set)**

A covered entity (Ferris State University) may use one of its own workforce to create the limited data set. The Department of Human Services also has indicated that a covered entity may allow a person requesting a limited data set to create it, as long as the person is acting as a business associate of the covered entity. A business associate is someone who is not part of the covered entity’s workforce but who will use the covered entity’s PHI to perform some task on behalf of the covered entity. Examples of business associates are Eagle Soft Software from the company Patterson Dental, lawyers and firms that analyze patient data, etc. The covered entity (Ferris State University) must enter into a separate
business associate agreement with the entity and the agreement must meet the requirements of the Privacy Regulations. Once the limited data set is created under the business associate agreement, all of the PHI, other than the PHI qualifying as the limited data set under the data user agreement must be returned to the covered entity.

It is possible that someone will act as the covered entity’s business associate to create the limited data set from a broader set of PHI. In such a case, the recipient will need to sign both a data use agreement and the business associate agreement.

**Responsibility for Data Use Agreements**

A. When Ferris State University (FSU) is the provider of the data:

FSU has drafted a data use agreement for use by those who wish to disclose limited data set to recipients.

B. When FSU is the recipient of the data:

If FSU is the recipient of limited data set of PHI from a non-FSU source, the recipient may be asked to sign the other party’s Data Use Agreement. In this case, the recipient is responsible for reviewing the Data Use Agreement and determining if it complies in material terms with the Data Use Agreement template. If the other party’s Data Use Agreement is significantly different from the FSU Data Use Agreement template, or if there is any uncertainty, the FSU Governmental Relations and General Counsel Division is to be consulted.

**Tracking and Accounting**

Disclosures of a limited data set are not subject to the HIPAA tracking/accounting requirements. The rationale appears to be that the marginal increase in privacy protections that such an accounting would provide is outweighed by its burdens. The Department of Health and Human Services has taken the position that the privacy of individuals regarding PHI disclosed in a limited data set can be adequately protected through a signed data use agreement.

**Disclosure** – Means releasing, transferring, providing access to, or divulging information in any manner outside the dental practice or other entity holding the information 45 CFR § 160.103

We do not sell personal health information or disclose it to companies that wish to sell a patient their products. We must have written permission (called an “authorization”) to use and disclose a patient’s health information, except for the uses and disclosures described below. Additionally, Michigan law may require that we obtain your specific prior authorization to use and disclose certain health information, such as behavioral health, substance abuse and HIV/AIDS information.

- **You and Your Personal Representative**. We may disclose your health information to you or your personal representative (an individual who has the legal right to act on your behalf).

- **Others Involved in Your Care**. We may share your health information with family members or friends who are directly involved in your medical care, or the payment of your medical care, when you are present and have given us verbal or written permission. We will not discuss your health information with your family or friends if you are not present unless you have given us
your permission or we believe it is in your best interest. Our health professionals will exercise their professional judgment in determining when friends and family members may receive health information (e.g., a family member picking up a prescription from the pharmacy for a sick individual).

- **Treatment.** We may use your health information or disclose it to third parties to aid with your medical treatment. We may disclose health information about you to doctors, nurses, pharmacists, technicians, medical students, or other persons who are involved in taking care of you. For example, if you are being treated for a knee injury, we may give your health information to the people providing your physical therapy. Similarly, we may notify your personal doctor about treatment you receive in an emergency room. Our pharmacies may use your health information for dispensing prescription medications to you.

- **Payment.** We may use your health information or disclose it to third parties, including the subscriber, in order to obtain payment for your medical treatment or prescription medications, to determine your eligibility for benefits, or to coordinate your benefits with other health plans. For example, we may discuss your health information with your doctor to obtain a prior approval for a medical procedure or to determine whether our health plan will cover the treatment. Similarly, we may use or disclose your health information to others to assist with adjudication of health claims or to coordinate benefits with other health coverage you may have. Also, we may share information with a medical provider to determine whether a particular treatment is medically necessary, experimental, or investigational. We will send to the member an explanation of benefits indicating the amount the health plan has paid for medical services provided to the member, his or her covered spouse and other covered dependents.

- **Health Care Operations.** We may use your health information and disclose it to third parties who help us with the day-to-day management of our health plan and our health care services, providers, and pharmacies. These uses and disclosures are allowed under HIPAA’s definition of Treatment, Payment, and Operations (TPO) and ensure that you receive quality care. For example, we may use your health information to conduct quality assessment and improvement activities, review the performance of our health plan (including our medical professionals and pharmacists), underwrite and rate premiums, conduct and arrange for medical review, legal services, and auditing activities, business planning and development, and other general health care delivery and health plan administration activities. However, we will not use your genetic information for any underwriting or eligibility purposes.

- **Appointment Reminders and Health Related Benefits and Services.** We may use and disclose your health information to remind you about prescription refills and appointments for medical/dental care in our offices.

- **Marketing.** We may also use and disclose your health information to tell you about health-related benefits or services available through our health plan that may be of interest to you, including communications about subsidized treatment options.

- **As Required By Law.** We will disclose your health information to third parties when required to do so by federal, state or local law. For example, we may share your health information when
required to do so by state workers’ compensation law, the Department of Health and Human Services, or state regulatory officials.

- **To Avert A Serious Threat To Health Or Safety.** We may use and disclose your health information to third parties when it is necessary to prevent a serious threat to your health and safety or to the health and safety of the public or another person. Any disclosure, however, would only be to someone able to assist in preventing the potential harm.

- **Lawsuits and Disputes.** If you are involved in a lawsuit or a dispute, we may disclose your health information in response to a court or administrative order. We may also disclose your health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only after we make efforts to inform you of the request or to obtain an order protecting the requested information. If you are a party to a lawsuit in a Michigan court case, a court order or your authorization must be provided to release your health records (in addition to a subpoena).

- **Public Policy Matters.** We may use or disclose your health information in certain limited instances for matters involving the public welfare, such as:
  - For public health risks (e.g., prevention or control of disease, reporting births and deaths, reporting abuse and neglect) or for research purposes when there are sufficient privacy protections in place.
  - To a health oversight agency for activities authorized by law (e.g. audits, investigations, inspections, and licensure necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws).
  - To law enforcement officials (in response to a court order, subpoena, warrant, summons or similar process or to report certain kinds of crimes) and to national security officials under certain limited circumstances.
  - To a funeral director, coroner, or medical examiner to permit them to carry out their duties
  - To facilitate organ donation and specified research purposes, so long as certain safety measures are in place to protect your privacy.

- **Employers and Plan Sponsors.** In order for you to be enrolled in a health plan, we may share limited information with your employer or other organizations that help pay for your health coverage. However, if your employer or another organization that helps pay for your health coverage asks for specific health information, we will not share your health information unless they first obtain your written authorization.

- **Business Associates.** We hire third parties to provide us with various services that are necessary for our health plan to function. Before we share your health information with these companies, we will have a written contract with them in which they promise to protect the privacy of your health information.
• **Other Uses and Disclosures of PHI.** We have no plans to use or disclose your health information for purposes other than those provided for above or as otherwise permitted or required by law. If you provide us an authorization to use or disclose your health information to third parties, you may revoke the authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information for the reasons covered by your written authorization. Please remember that we are unable to take back any disclosures we have already made with your authorization.

**Health Care Operations** – This is a “broad” category of dental practice activities such as business management and general administrative activities of the dental practice (for example, HIPAA compliance, customer service, resolving internal grievances, the sale of the practice to another covered entity (or to an entity that will become a covered entity following the sale) and due diligence related to the sale, and de-identifying PHI). Other examples include business planning and development (such as cost management and planning related analyses), conducting quality assessment and improvement activities, certain patient safety activities, case management and care coordination, reviewing the competence or qualifications of health care professionals, conducting training programs in which health care students, trainees, or practitioners learn under supervision, training of non-health care professionals, licensing and credentialing activities, arranging for legal services, and auditing (including fraud and abuse detection and compliance programs). To determine whether an activity is a health care operation, consult the full definition in 45 CFR § 160.103.

**Minimum Necessary** – When a dental practice uses or discloses patient information or requests patient information from a health care provider, health plan, clearinghouse, or business associate, the dental practice must make reasonable efforts to limit the patient information to the minimum amount necessary.

Exceptions: Minimum necessary does NOT apply in the following situations:

• Disclosing patient information to a health care provider for treatment purposes
• Requesting patient information from a health care provider for treatment purposes
• Disclosing a patient’s information to the patient or personal representative
• When a patient has signed an authorization form for the use or disclosure
• Disclosures to the U.S. Department of Health and Human Services (HHS)
• Uses and disclosures required by law
• Uses and disclosures required in order to comply with the Privacy Rule

A dental practice may not access, use, disclose or request a patient’s entire dental record unless the entire dental record is needed to accomplish the purpose of the use, disclosure, or request, or unless one of the above exceptions applies.

**Office of Civil Rights** – a.k.a., OCR
**Payment** – Generally means the dental practice’s activities to obtain reimbursement or compensation for service performed or products provided and a health plan’s activities to collect premiums, determine the plan’s responsibility to provide coverage and benefits, and provide coverage and benefits. Examples of “payment” activities include things like determination of eligibility or coverage, coordination of benefits, determination of cost sharing amounts, billing, claims management, collection activities, review of medical necessity, coverage, appropriateness of care or justification of charges, utilization review, including precertification and preauthorization, concurrent and retrospective review of services, and disclosure of limited information to consumer reporting agencies relating to collection of premiums or reimbursement (names and addresses, date of birth, Social Security number payment history, account number, and name/address of health care provider and/or health plan). 45 CFR § 164.501.

**Protected Health Information or PHI** – Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media and includes information transmitted or maintained in any other form or medium. The abbreviation “PHI” in this manual is intended to mean “protected health information” (“PHI”). Most patient information is PHI, including dental records, health histories, billing records, radiographs, full-face photographs, and even “demographic” information such as patient names, addresses, phone numbers, email addresses, genders, etc.

**Patient** – The HIPAA rules refer to “individuals.” For a dental practice, this usually means the patient and that term is used in this manual. HIPAA protects information about both current and former patients, and that in some cases other people, such as a patient’s legal representative, or the parents or guardians of minor children, have rights under HIPAA.

**Use** – We have no plans to use or disclose health information for purposes other than those provided by law. If a patient provides an authorization to use or disclose health information to third parties, that authorization may be revoked, in writing, at any time. If authorization is revoked, Ferris State University will no longer use or disclose the patient’s health information for the reasons covered by the written authorization. Ferris State University is unable to take back any disclosures already made with a patient’s authorization.

**Workforce Employee** – The FSU dental hygiene clinic workforce employee means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a dental practice, is under the direct control of the dental practice, whether or not they are paid by the dental practice. A business associate’s workforce means the business associate’s employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the business associate, is under the direct control of the business associate, whether or not they are paid by the business associate. 45 CFR § 160.103.
INTRODUCTION

On January 25, 2013, the federal government published changes to the HIPAA rules that require covered dental practices (such as the Ferris State University Dental Hygiene Clinic, a.k.a. dental practice) to update compliance programs.

Effective and Compliance Dates

The changes are effective March 26, 2013, but dental practices have until September 23, 2013 to come into compliance.

All business associate agreements entered into on or after January 25, 2013 must be compliant with the new requirements by September 23, 2013, but a transition period until September 22, 2014 applies to certain agreements that were in place on January 25, 2013.

The increased civil money penalties have been in effect since 2009, and apply to HIPAA violations occurring on or after February 18, 2009.

HISTORY

Purpose of the Law

Congress passed the HIPAA law in 1996 to require national standards for electronic health care transactions and code sets. Since Congress recognized that advances in electronic technology could erode the privacy of health information, Congress added provisions to the law requiring Federal privacy protections for patient health information. These provisions led the government to adopt the HIPAA Security and Privacy Rules. The rules have been strengthened over time. For example, the 2009 HITECH ACT required the Breach Notification Rule and other enhancements to HIPAA that were intended to enhance public confidence in the privacy of patient information as health care providers increased their use of electronic health record (EHR’s). Many of the HITECH enhancements are embodied in new regulations issued on January 25, 2013 (“the Final Rule”).

Compliance Dates

Dental practices were required to comply with the Privacy Rule beginning in 2003. Security Rule compliance began in 2005. In 2009, the Breach Notification Rule came along, and the government increased penalties for HIPAA violations and strengthened HIPAA enforcement.
State Law

A dental practice’s HIPAA program must comply with both HIPAA and applicable state law. If a state is not contrary to HIPAA, a dental practice must comply with both HIPAA and the state law. If a state law is contrary to HIPAA, a dental practice must comply with the state law if the state law is “more stringent” than HIPAA. In general, state law is more stringent than HIPAA if the state law relates to the privacy of patient information and provides greater privacy protection for patient information or greater rights to patients with respect to that information.

For example, HIPAA requires a dental practice to act within 30 days if a patient asks to see or get copies of certain patient information. If state law requires a dental practice to act on such a request in a shorter time frame, it would be more stringent than HIPAA.

Ferris State University Dental Hygiene Clinic has a qualified attorney(s), both on campus and within the state of Michigan to make sure the dental practice’s HIPAA compliance program is compliant with both HIPAA and applicable state laws.

Enforcement

Federal government enforcement of HIPAA used to be complaint driven. For example, if a patient complained to the federal government that a dental practice was not complying with HIPAA, the government could investigate and could impose penalties or corrective action. While this is still the case, the federal government now has expanded enforcement responsibilities and has the authority to conduct HIPAA audits that are not generated by a patient complaint or other information indicating possible noncompliance. The federal government may also investigate breaches that are reported to the US Department of Health and Human Services (HHS) in accordance with the Breach Notification Rule. The Office for Civil Rights, an agency of HHS, is responsible for federal HIPAA enforcement.

In addition to federal enforcement, the HITECH Act of 2009 gave state attorneys general the authority to bring civil actions on behalf of state residents for violations of the HIPAA privacy and Security Rules. State attorneys general have the authority to obtain damages on behalf of state residents and to enjoin further violations of the HIPAA Privacy and Security Rules. More information can be found at www.hhs.gov/ocr/privacy/hipaa.

Penalties

In the beginning, civil money penalties for a dental practice that did not comply with HIPAA were limited to $100 or less per violation, up to an annual cap of $25,000 for all violations of the same HIPAA requirement or prohibition. Today, there are tiered penalty amounts for increasing levels of culpability, up to an annual cap of $1.5 million for all violations of the same HIPAA requirement or prohibition. If a violation was due to willful neglect and was not corrected within 30 days, there is a minimum penalty of $50,000 per violation.

Applies to: All covered entity dental practices of which Ferris State University Dental Hygiene Clinic is a covered entity.
Effective date: The increased penalties apply to HIPAA violations occurring on or after February 18, 2009

Background:

OCR has the right to impose civil money penalties on dental practices that violate HIPAA. Some HIPAA violations carry criminal penalties, including fines and imprisonment. OCR also has the authority to require a dental practice to take corrective action, including instigating a formal (and costly) Corrective Action Plan if OCR finds the dental practice noncompliant.

The new rule has tiered penalty amounts for increasing levels of culpability, up to an annual cap of $1.5 million for all violations of the same HIPAA requirements or prohibition. If a violation was due to willful neglect and was not corrected within 30 days, there is a minimum penalty of $50,000 per violation.

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Penalty Range Per Violation</th>
<th>Maximum Penalty for All Such Violations of Identical Provisions in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Reasonable cause</td>
<td>$1,000 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful neglect, timely corrected</td>
<td>$10,000 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful neglect, not timely corrected</td>
<td>$50,000</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>

How violations are counted.

If a HIPAA violation continues for a number of days, (for example, if appropriate safeguards are lacking for a number of days), the number of identical violations may be counted on a PER DAY BASIS. OCR considers the number of affected individuals and HIPAA requirements violated. For instance, usually with a breach of unsecured patient information there will be both (1) an impermissible use or disclosure and (2) a safeguards violation, and OCR may calculate a separate civil money penalty for each. As such, a dental practice may be liable for multiple violations of multiple requirements, up to a cap of $1.5 million for EACH requirement.

Aggravating and mitigating factors.

HIPAA contains a list of aggravating and mitigating factors that can affect the amount of civil money penalty. The new rule requires the government to consider the factors when determining the amount of a penalty for a HIPAA violation.

The OCR will determine the amount of a penalty on a case-by-case basis, depending on the nature and extent of the violation and the nature and extent of the resulting harm, as well as other aggravating and mitigating factors listed in 45 CFR 160.408. Examples of the factors include:
• The number of individuals affected

• Whether the violation caused physical, financial, or reputational harm or hindered a patient’s ability to obtain health care

• The dental practice’s history of prior compliance or non-compliance

• The financial condition of the dental practice

• Whether the imposition of civil money penalty would jeopardize the dental practice’s ability to continue to provide health care.

• The size of the dental practice
POLICY STATEMENT


FERRIS STATE UNIVERSITY DENTAL HYGIENE CLINIC OR PARTIES EMPLOYED OR INVOLVED IN ACADEMIA RELATED TO DENTAL HYGIENE PATIENT CARE AND THE DENTAL HYGIENE CLINIC WILL NOT DISCLOSE PROTECTED HEALTH INFORMATION TO NON-HEALTH CARE ENTITIES WITHOUT A SIGNED PATIENT AUTHORIZATION OR OTHER HIPAA PERMISSION FORMS. FERRIS STATE UNIVERSITY DENTAL HYGIENE CLINIC WILL INSTITUTE APPROPRIATE SAFEGUARDS TO PREVENT IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION.
PRIVACY AND SECURITY
POLICIES AND PROCEDURES
FOR
HIPAA

(HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT)

It is not called HIPPO!

I. PRIVACY OFFICER 45 CFR 164.530 (a) & 45 CFR 164.524 (e) (2)

POLICY:

Our dental practice’s Privacy Officer shall be responsible for developing and implementing our HIPAA privacy and breach notification policies and procedures, receiving complaints about our privacy and breach notification practices, providing further information about our Notice of Privacy Practices, and receiving and processing requests for access, amendment, and accountings of disclosure.

(See Privacy Officer Job Description in Appendix, page 69)

PROCEDURE:

Staff Duties – Our Privacy Officer is responsible for developing privacy and breach notification policies and procedures and putting them into action. Examples of these policies and procedures include how to protect patient privacy, how you are permitted to use, disclose and request information about patients, and how to respond to requests from patients and others concerning dental records and other information.

Privacy Officer Duties – The Privacy Officer is responsible for developing and implementing privacy and breach notification policies and procedures and updating them as appropriate. The policies and procedures will apply to patient information in oral, written and electronic form. Your duties include, but are not limited to, the responsibilities in the Privacy Officer job description (see Appendix).
II. PRIVACY POLICIES AND PROCEDURES (45 CFR 164.530 (i))

POLICY:

Our dental practice will develop and implement policies to comply with the HIPAA Privacy and Breach Notification Rule, as well as applicable state laws. We will revise our policies and procedures promptly as appropriate when there is a change in the law or in our privacy practices.

PROCEDURE:

Staff Duties – Our dental practice has privacy and breach notification policies and procedures. The policies and procedures will be updated from time to time. All workforce members must comply with the policies and procedures when they do their job.

Privacy Officer Duties – this person is responsible for developing, implementing and documenting our privacy and breach notification policies and procedures and for updating them as necessary – for example, if our privacy practices change, if the HIPAA rules change, or if there is a change in state law.

Provide all members of our workforce with a paper or electronic copy of the privacy, security and breach notification policies and procedures, and any revisions, and keep a current copy readily accessible to all workforce members.

When there is a change in the law or in our privacy practices, revise the policies and procedures (and if necessary, the Notice of Privacy Practices) as appropriate prior to the effective date of change.

(See Sample of the Acknowledgment of Receipt of HIPAA Policies and Procedures in Appendix, page 72)
III. NOTICE OF PRIVACY PRACTICES OR NPP 45 CFR 164.520, 45 CFR 164.530 (i), & 45 CFR 164.502 (i)

POLICY:

Our practice will provide a notice of our privacy practices to our patients, and to anyone else who requests a copy. Our Notice and the way we provide it will comply with HIPAA and applicable state law. Our practice will revise the Notice as appropriate, and will provide the revised Notice as required by HIPAA. Our practice will not use or disclose patient information in a manner that is inconsistent with our Notice, HIPAA, or state law.

PROCEDURE:

Staff Duties – Our Notice of Privacy practices describes how our dental practice may use and disclose patient information. Ask the Privacy Official if you have any questions about the Notice. Do NOT use or disclose patient information in violation of our Notice.

Provide our Notice to each new patient at his or her first appointment, and ask the patient to sign the Acknowledgement of Receipt form for patients. (See Appendix for sample of Acknowledgment of Receipt form for Patients). If a patient refuses to sign the acknowledgment of receipt, note on the form that you tried to get the acknowledgment, and the reason that you could not do so. If the patient has a personal representative, such as the parent or guardian of a minor, provide the Notice to the personal representative and ask the personal representative to sign the acknowledgment form.

Retain each completed acknowledgment form for six (6) years from the date it was created or the date that it was last in effect, whichever is later. If we don’t have an acknowledgment form for a patient, then at that patient’s next appointment give the patient a copy of the Notice and ask the patient to sign the acknowledgment.

We have a supply of Notices at the reception desk for people who ask for a copy to take with them. Give a copy to anyone who asks for one.

However, inmates do not have a right to a Notice of Privacy Practices. An inmate is defined as a person who is incarcerated in or otherwise confined to a correctional institution.

Privacy Officer Duties – This person is responsible for developing our Notice of Privacy (and/or working with appropriate IT staff, administrators, lawyers, consultants on campus) and for revising our Notice when appropriate – for example, if our privacy practices change, if the HIPAA rules change, or if there is a change in the state law.

Providing the Notice – the Privacy Officer is responsible for training workforce members to provide the Notice, for posting a copy of the Notice in a clear and prominent place in the dental practice, for making sure there is a supply of Notices at the reception desk for people who ask for a copy to take with them, and for posting the Notice prominently on our practice’s website and making it available electronically on our website.

Revising the Notice – The Privacy Officer is responsible for the following:
1. Whenever our privacy practices change, or there is a change in the law or the HIPAA Rules that requires a change to the Notice, determine whether our dental practice must revise the Notice. If so, revise the Notice as appropriate.

2. If our Notice is revised, then on or after the effective date of the revision, our practice will:

   - Provide the new Notice to new patients on their first appointment and ask them to sign the acknowledgment.
   - Have a supply of copies of the new Notice available in the dental office and give a copy to anyone who asks for a copy to take with them.
   - Post the new Notice in a clear and prominent location in the dental office.
   - Post the new Notice on our website, and make the new Notice available electronically through the website.
   - Retain at least one copy of both the old and the new Notices for at least six (6) years from the date when the document was created, or the date when the document last was in effect, whichever is later.

**Complying with our Notice.** Train workforce members to comply with our Notice.

*(See Notices of Privacy Practices in Appendix, page 73)*
IV. DESIGNATED RECORD SETS 45 CFR 164.501, 45 CFR 164.524, & 45 CFR 164.526

POLICY:

Our Privacy Officer will create and retain a written list of our dental practice’s “designated record sets”, and will update the list whenever it is appropriate.

(See Designated Record Set for FSU Dental Hygiene Clinic in Appendix, page 80).

PROCEDURE:

Privacy Officer Duties – The Privacy Officer will create a list of every set of records in our dental practice that meets the HIPAA definition of a “designated record set”. The list must include

1. All dental records and billing records about patients maintained by or for our dental practice.

2. Every group of records maintained by or for our dental practice that is used, in whole or in part, by or for our dental practice to make decisions about patients.

Note: a “record” means any item, collection, or grouping of information that includes patient information and is maintained, collected, used, or disseminated by or for our dental practice. Our designated record sets that are maintained off-site and/or by a business associate must be included on the list.

Whenever our dental practice changes its recordkeeping system in a way that changes our list of designated record sets create a revised list of designated record sets. Retain each list for at least six (6) years from the date when it was created, or from the date when it was last in effect, whichever is later.
V. **MINIMUM NECESSARY 45 CFR 164.502 (b) & 45 CFR 164.514 (d)**

**POLICY:**

Our dental practice will use, disclose and request the minimum amount of patient information that is necessary for the intended purpose of the use, disclosure or request.

**PROCEDURE:**

**Staff Duties** – Do not access patient information that you are not authorized to access and is not necessary to do your job. Accessing the patient information out of curiosity or for other impermissible purposes is prohibited, and will result in disciplinary action. When making a routine disclosure or request, follow our dental practice’s written minimum necessary limits. Before our dental practice makes a non-routine disclosure or requests, we must assess the minimum necessary patient information for the purpose. Always limit uses, disclosures and requests for patient information to the minimum amount necessary for the purpose.

**Privacy Officer Duties** – Develop the following documents and keep them up to date:

The minimum necessary patient information that our workforce members are authorized to access to do their jobs

*(See Workforce Access to Patient Information List in Appendix, page 82 & 84)*

**Action Items Needing to Be Done to Accomplish Minimum Necessary:**

- Workforce members within the dental practice have been identified by category, patient information needed to do their jobs, and any conditions that apply to their access.

- Routine Disclosures and Requests will be managed by the form called Routine Disclosures and Requests and can be found in the Appendix. This form is to be used whenever our practice makes a routine disclosure of patient information to a third party, or for use when our dental practice makes a routine request for patient information from a third party. The form is self-explanatory regarding the required information.

- Occasionally, the dental practice may want to disclose or request patient information in a non-routine situation. Our dental practice will assess non-routine disclosures and requests to determine the minimum amount of information that is necessary for the purpose. This determination will most likely involve the Clinic Clerks and the Privacy Officer.

*(See Routine Disclosures and Requests Form in Appendix, page 90)*
Minimum Necessary when Responding to Requests for Patient Information

In most cases the dental practice will determine the minimum necessary information to disclose when responding to an appropriate request for patient information, and may not rely on the person requesting the information to determine the minimum necessary amount. However, in the following situations, the dental practice may rely on the person making the request to determine the minimum necessary amount, when it is reasonable to do so under the circumstances:

- The dental practice is making a permitted disclosure to a public official and the public official tells the dental practice that the information requested is the minimum necessary for the stated purpose.

- A health care provider, health plan, or health care clearinghouse that is a HIPAA covered entity is asking for the patient information.

- A professional who is a member of the dental practice’s workforce, or who is a business associate of the dental practice, requests patient information in order to provide professional services to the dental practice, and the professional tells the dental practice that the information requested is the minimum necessary for the stated purpose.

- The dental practice wishes to disclose patient information for certain research purposes and the documentations and representations required in section 45 CFR 164.512 (i) of the Privacy Rule are in place.
VI. VERIFICATION OF IDENTITY 45 CFR 164.514 (h)

POLICY:

Our dental practice will not disclose patient information to persons who do not have the authority to access the information.

PROCEDURE:

Staff Duties – If a person asks you for information about a patient, and you know the person and know that the person has the authority to get the information such as date of birth, address, or approximate date of last appointment. If you are unsure, direct the request to the Privacy Official.

In all other cases, if a person asks for patient information and you do not know the person, or you are not sure that the person has the authority to access the information requested, direct the request to the Privacy Official who will verify the person’s identity and authority to get the patient information requested.

Privacy Officer Duties – If a person asks for information about a patient, and we do not know the person and/or we are not sure that the person has the authority to access the information they asked for, the Privacy Official is responsible for verifying the person’s identity and authority to get the patient information they request. Determination will be made as follows:

- Is the disclosure required or permitted?
- Did the patient sign an authorization form before our dental practice makes the disclosure?
- The minimum necessary information is provided, where applicable?

If a person we don’t know comes to the dental office and asks for information about a patient, check the person’s photo ID and any other appropriate documentation and do the following:

- If the person claims to be a patient asking for his or her own information, ask for the date of birth, address, approximate date of last appointment, or some other information to verify identity. If the person wants to see or get copies of his or her own information, or a personal representative wants to see or get copies of the patient’s information, refer to the section in this manual about Patient Rights and Requests.

- If the person says that he or she is a family member or friend of the patient, ask to see a photo ID and refer to the section in this manual about disclosures to friends or family members.

- If the person says that he or she is a patient’s personal representative, ask to see a photo ID and exercise professional judgment to verify that the person is acting on behalf of the patient. Where appropriate, require the person to provide documentation, such as proof of legal guardianship or a Power of Attorney (they usually have these documents with them).
• If the person is a public official, ask to see his or her identification badge or other credentials. If the request is in writing, review the government letterhead, insignia, address, and credentials.

If confronted with any of the following situations, check the special rules for verifying identity in 45 164.515 (h) and consult legal counsel as appropriate:

• If a public official asks for patient information

• If the dental office receives an administrative request, subpoena, or summons, civil or authorized investigative demand, or similar process

• If the dental office receives a request for patient information for research purposes.

**NOTE:** If all procedures have been followed for verification and you do not believe that our dental practice should provide patient information to the person asking for it, politely tell the person that we are unable to release the information. The person may submit a request in writing and provide more information about his or her identity and authority to get the information.

Require all persons, other than patients we know, personally and their family members and friends as is needed to complete the Verification of Identity Form.

This form is to be maintained for six (6) years from the date the document was created, or six (6) years from the date the document was last in effect, whichever is later.

*(See Verification of Identity Form in Appendix, page 92)*
VII. **REQUIRED DISCLOSURES 45 CFR 164.502 (a) (2)**

**POLICY:**

Our dental practice will disclose patient information when required by HIPAA. The Standard is detailed below:

The Standard: Disclosures by whistleblowers and workforce member crime victims.

1. Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

   The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers or the public; and

   The disclosure is to:

   A. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

   B. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

2. Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

   The protected health information disclosed is about the suspected perpetrator of the criminal act; and

   The protected health information disclosed is limited to the information listed in 164.412 (f)(2)(i).

**PROCEDURE:**

**Staff Duties** – Refer all of the following requests to the Privacy Officer:

- If a patient, or a patient’s personal representative, asks to see or get copies of the patient’s information

- If a patient, or a patient’s personal representative, asks for an accounting of disclosures
• If HHS asks for patient information

**Privacy Officer Duties** – HIPAA requires a dental practice to disclose patient information in response to an appropriate request from a patient or personal representative to see or get copies or for an accounting of disclosures. Disclosure is also required when patient information is requested by HHS in connection with a HIPAA investigation, compliance review, or audit. In these situations, patient authorization is not required, and the minimum necessary requirement does not apply. However, certain steps in Request for Access and Accounting of Disclosures must be followed.

*See the ADA Practical Guide to HIPAA Compliance Privacy and Security in Appendix, page 93*
VIII. PERMITTED USES AND DISCLOSURES, Reference Listed Below

POLICY:

Our dental practice will not use or disclose patient information without written authorization unless the use or disclosure is required or permitted under HIPAA.

PROCEDURE:

Staff Duties – Do not use or disclose patient information, except for routine purposes that you are authorized and trained to make, unless you have the prior approval of the Privacy Officer.

Privacy Officer Duties – Will be responsible for determining whether a proposed use or disclosure of patient information requires the patient to sign an authorization form, or whether the use or disclosure is permitted by HIPAA.

Policies and procedures will continue to be developed for handling these situations that are likely to arise in our dental practice. Officer will train staff and put the policies and procedures into action.

References to these rules can be found in:

45 CFR 164.502(a) (i)
45 CFR 164.502 (g)
45 CFR 164.510 (b)(5)
45 CFR 164.502 (f)
45 CFR 501 (definition of “treatment”)
45 CFR 164.502 (a)(1)(ii)
45 FR 164.501 (definition of “payment”)
45 FR 164.506
45 FR 164.501 (definition of “health care operations”)
45 FR 164.506
45 CFR 164.502 (a)(1)(iii)
45 CFR 164.510
45 CFR 164.502 (e)
45 CFR 164.502 (j)
45 CFR 164.512 (f)(2)
45 CFR 164.502 (d) (de-identification)
45 CFR 164.514 (e)(limited data sets)
45 CFR 164.514(f)
45 CFR 164.14 (e)(f)
45 CFR 164.502 (d)

See Decision Tree: Decedent PHI in Appendix, page 94
IX. PATIENT AUTHORIZATION FORMS 45 CFR 164.508

POLICY:

Our dental practice will not use or disclose patient information without having the patient sign an appropriate authorization form unless the Privacy Rule permits or requires the use or disclosure.

PROCEDURE:

Staff Duties – Consult the Privacy Officer before using or disclosing patient information unless the use or disclosure is routine and you are authorized to make the use or disclosure.

Privacy Officer Duties – The privacy officer will train workforce members to recognize routine uses and disclosures that they are authorized to make and that are required or permitted by HIPAA, including uses and disclosures for purposes of treatment, payment and healthcare operations. If the state of Michigan requires patient consent for certain uses and disclosures, train workforce members to use the appropriate consent forms when required.

If the dental practice wishes to make a use or disclosure of patient information that is not permitted or required by HIPAA, the patient must first sign an authorization form.

Do the following 4 things when a signed authorization form is required:

1. Determine whether the dental practice’s standard authorization form is sufficient, or whether additional information should be included on the form (for example, authorizations for subsidized marketing communication or for the sale of patient information require additional information on the form). Properly fill in all of the appropriate blanks on the form.

2. Verify identification if you do not personally know the person who will sign the authorization form, or if you are not sure the person is authorized to sign it (for example, if you are not sure that the person is a personal representative of a patient). Do not permit an unauthorized person to sign an authorization form.

3. Give the authorization form to the patient and let the patient read it and ask questions. Answer any questions the patient may have about the form. If the patient understands and agrees with the form, have the patient sign the form and return to you.

4. Confirm that the authorization is properly completed and signed, and make sure that the following information is in the form:
   - A description of the patient information to be used or disclosed
   - The name of the person(s) authorized to make the disclosure
   - The name of person(s) to whom the dental practice may disclose the information
   - The purpose for the use or disclosure (if the patient initiated the authorization you may write “at the request of the individual” in this space)
• An expiration date or an expiration event that relates to the patient or to the purpose of the disclosure

• Signature and date of signature of the patient or the patient’s personal representative. If the authorization is signed by a patient’s personal representative, the form must have a description of the representative’s authority to act for the patient

**Defective authorization.** An authorization is defective and is not valid if:

• It has expired

• The required information has not been filled out completely

• Our practice knows that the authorization has been revoked

• Our practice knows that material information in the authorization is false

5. Give the patient a copy of the completed, signed authorization form. Retain the authorization form for at least six (6) years from the date of its creation, or from the date when it was last in effect, whichever is later.

*(See AUTHORIZATION FORM FOR USE OR DISCLOSURE OF PATIENT INFORMATION - CORE ELEMENTS in Appendix, page 95)*
X. **SUBSIDIZED MARKETING COMMUNICATIONS 45 CFR 164.501 (definition of “marketing”) & 45 CFR 164.508 (a) (3)**

**POLICY:**

Prior to making a marketing communication, our dental practice will obtain any required written authorization, as needed.

**PROCEDURE:**

**Staff Duties** – Unless approved, do not:

- Use or disclose patient information for making a communication that encourages someone to buy or use a product or service
- Encourage patients to buy or use a product or service, or
- Accept payment from anyone for making a communication that encourages someone to buy or use a product or service.

Only the DH Department Head, the Program Coordinator, and the DH Clinic Operations Supervisor, along with appropriate individuals within the university, may approve subsidized marketing communications.

**Privacy Officer Duties** – Before the dental practice accepts financial remuneration (dollars) for making a communication encouraging someone to buy or use a product or service, or uses or discloses patient information for making such a communication, determine:

1. Whether the communication meets the definition of a “marketing communication”
2. Whether the communication is for a permissible purpose under HIPAA (such as treatment, case management, care coordination, or health plan benefits), and
3. Whether the patient’s written authorization is required

If patient authorization is required,

1. Develop an appropriate authorization form that includes a statement that financial remuneration is involved, and
2. Ensure that each patient signs the form before his or her information (including name and address) is used or disclosed for purposes of making the communication

In the following situations, a communication can be made without written authorization from the patient, even if the dental practice will receive financial remuneration, as long as the communication is for a permissible purpose under HIPAA

- In person face-to-face communications
- Promotional gifts of nominal value

- When the dental practice receives only non-financial or in-kind remuneration for making a communication for a permissible purpose under HIPAA

- Refill reminders or other communications about a drug or biologic that is currently being prescribed to the person, but only if the payment received by the dental practice is reasonably related to the dental practice’s cost of making the communication
XI. SALE OF PATIENT INFORMATION 45 CFR 164.502 (a) (5) (ii) & 45 CFR 164.508 (a) (4)

POLICY:

Our dental practice will NOT “sell” patient information (as defined by HIPAA). It is not our practice to “sell” patient information to any vendor, clearinghouse, etc.

PROCEDURE:

Staff Duties – The DH staff and are prohibited from exchanging any information about our patients for money or anything else of value. “Information about our patients” includes patient lists, schedules, names and addresses, and any other information about our patients. “Anything of value” includes money, things, opportunities, information, or anything else that has even a small amount of value.

Privacy Officer Duties – Will train staff to NOT “sell” or disclose any patient information in exchange for anything of value, or permits a business associate to do so. The Privacy Officer will follow the HIPAA rule and train staff according to 45CFR 164.502(a)(5)(ii).

Authorization forms (Use or Disclosure of Patient Information) will NOT be needed for this policy because Ferris State University Dental Hygiene Clinic does NOT permit the sale of any patient information.
XII. MITIGATES HARM (45 CFR 164.530 (f))

POLICY:

If our dental practice or one of our business associates uses or discloses patient information in violation of its privacy policies and procedures or in violation of the Privacy Rule, our Ferris State University General Counsel may decide to mitigate, to the extent practicable, any harmful effect known to us.

PROCEDURE:

Staff Duties – Immediately tell the Privacy Officer about any improper use or disclosure of patient information by our dental practice or by one of our business associates. If you are aware of any harmful effects of the improper use or disclosure, or any ways to lessen those harmful effects, tell the Privacy Official immediately.

Privacy Officer Duties – When it has been discovered that our dental practice or one of our business associates has used or disclosed patient information in violation of its policies and procedures, or in violation of the Privacy Rule:

- Determine whether our dental practice is aware of any harmful effects of the use or disclosure
- If so, determine whether our dental practice is reasonably capable of doing anything capable to lessen the harmful effects
- Consults with FSU General Counsel for guidance when handling harmful effects
- Comply with the Breach Notification Rule and, if appropriate, log the use or disclosure in case the patient asks for an accounting of disclosures.

Remember that if our dental practice knows that a business associate is doing something that violates the business associate agreement, you must:

- Determine whether it is a “material” breach of the agreement (for example, it is likely a material breach if a business associate that does not provide the dental practice timely notice of a breach of unsecured patient information).
- If the breach is material, our dental practice must plan and take reasonable steps to end the violation
- And, if those steps are not successful, terminate the agreement with the business associate, if it is “feasible” to do so (for example, it may not be “feasible” to end an agreement with a business associate at that time if there is not another person or company that could take over the business associate’s responsibilities).
XIII. BUSINESS ASSOCIATES 45 CFR 160.103, 45 CFR 164.502 (e), 45 CFR 164.504 (e), 45 CFR 164.308 (b) & 45 CFR 164.314 (a)

POLICY:

Our dental practice will manage our relationships with business associates in compliance with HIPAA, and will not permit a business associate to access patient information unless a compliant business associate agreement is in place.

PROCEDURE:

Staff Duties – Do not permit outside persons or entities, such as contractors, vendors and consultants, to access patient information unless the person or entity is not a HIPAA “business associate”, or an appropriate business associate agreement is in place. In general, you may provide patient information to another health care provider for treatment purposes (for example, a specialist, dental lab, or pharmacy).

Notify the Privacy Officer IMMEDIATELY if you have reason to suspect that a business associate agreement is required but not in place, or that a business associate may be in violation of HIPAA.

Privacy Officer Duties – Will consult with FSU General Counsel and develop a Business Associate Agreement form from the current template provided by FSU General Counsel and update the form as appropriate.

In addition, the Privacy Officer will ensure that a compliant business associate agreement is in place for every business associate.

If our dental practice becomes aware that a business associate is in violation of HIPAA, then our practice must:

- Take reasonable steps to end the violation, and if that is not successful,
- Determine whether it is feasible to terminate the business associate agreement
  - a. If feasible, terminate the agreement
  - b. If not feasible, develop a project plan for bringing noncompliant business associate into compliance, or replacing the business associate as soon as is reasonably feasible
- Take reasonable steps to mitigate (lessen) any harm caused by the violation as recommended by FSU General Counsel

(See template of Business Associate Agreement provided by FSU General Counsel in Appendix, page 97 & 107)
XIV. PATIENT RIGHTS AND REQUESTS 45 CFR 164.524

POLICY:

Our dental practice will provide patients, and their personal representatives as appropriate, access to patient information in a designated record set as required by HIPAA.

PROCEDURE:

Staff Duties – If anyone asks to see or get a copy of patient information, politely tell the person that all requests must be in writing and must be viewed by the Privacy Official. Give the person a copy of our Request for Access form, ask them to fill it out and give it to the Privacy Official.

Privacy Officer Duties – Review requests for access. Promptly review all completed Request for Access forms to determine whether the request should be granted or denied in compliance with HIPAA. Access (or written denial of access) must be provided within 30 days of the date that our dental practice received the written request for access, unless our dental practice has properly extended the period for up to 30 additional days.

Verify the identity of the person making the request where appropriate.

If our dental practice believes there are permissible grounds to deny access, determine whether the grounds are appropriate and, if so, prepare and send the Denial of Request for Access form. It is prudent to work with FSU General Counsel when denying a request for access. If the grounds are denial are reviewable and the patient or personal representative requests a review, provide an appropriate review of the denial in compliance with HIPAA.

If our dental practice will grant a request to see records, arrange for a time and place in the dental office for the person to see the records within the appropriate time frame (within 30 days of the date that the dental practice received the request, or within the extension time period if properly extended).

If our dental practice will grant a request for copies of records, provide the copies within the appropriate time frame (within 30 days of the date that the dental practice received the request, or within the extension time period if properly extended).

Fee Schedule. If our dental practice decides to charge for copies (depending on the size of the document), .05 per copy may be charged for copying. The patient may have to assume the cost of mailing the copies. This may also include the cost of preparing summaries and explanation of patient information. The fee schedule must comply with both HIPAA and applicable state laws. For electronic copies, the patient may have to assume the cost of CD-ROMs and/or USB drives.

Electronic Copies. If a patient requests an electronic copy of a record that our dental practice maintains in an electronic designated record set, our dental practice must provide an electronic copy. Our dental practice is not required to provide the exact kind of electronic copy that the patient asks for if we cannot readily do so. If the patient does not agree to the kind of electronic copy that our dental practice can readily produce, offer the patient the information in hard copy.
Do **NOT** use outside electronic media in our system. Instead, we will have a supply of blank CD-ROMs and USB drives on hand to use to provide copies of patient information.

A patient has the right to ask for the electronic copy through email. If the patient prefers an **unencrypted email**, our dental practice must send the information in an unencrypted email. Our Request for Access form includes a notice that there is risk that the information in an unencrypted email could be read by a third party. Use reasonable safeguards to make sure that our dental practice correctly enters the email.

*(See Request for Access form in Appendix, page 117)*
AMENDMENT 45 CFR 164.526 (XIV CONTINUED)

POLICY:

A patient, and a personal representative, as appropriate, has the right to ask our dental practice to amend information about the patient in a designated record set if they believe that the information is not correct. As stated in our Notice of Privacy Practices (NPP), the request must be in writing and must give the reason for the amendment. If we deny the request, we will put our reason for denying the request in writing. If we agree to make the amendment, we will amend the record and tell the patient. If another HIPAA covered entity (such as a dental plan or a specialist) tells our practice that they made amendments to information about a patient, we will make the amendment to information in our designated record set, as appropriate.

PROCEDURE:

Staff Duties – If a patient (or patient’s personal representative) asks to amend any information in our dental practice’s records, politely tell them that the request must be in writing and give them a copy of the Request for Amendment form. Ask the patient to complete the form and give it to the Privacy Official. Only the privacy Official may receive and process requests for amendments. Immediately report a request to the Privacy Official.

Privacy Officer Duties - The Privacy Officer is responsible for receiving and processing all requests to amend the patient records.

Requests to amend patient records must be made in writing using our Request for Amendment form. The request must include a reason for the amendment. Make sure our Notice of Privacy Practices states that requests to amend records must be in writing and must state the reason for the request.

Review each requested amendment and determine whether the request should be approved or denied.

If our dental practice approves the amendment, append the amendment to the record, tell the patient that the amendment is approved, ask the patient who needs to be told about the amendment, ask the patient to agree that the dental practice may tell these persons about the amendment, and make a reasonable effort to send notice of the amendment within a reasonable time to the persons identified by the patient and to any other persons that we know have the information that we amended and may have relied on it (or may rely on it in the future) in a way that could harm the patient or put the patient at a disadvantage.

If our dental practice denies the amendment, send a written denial to the patient that contains the information required by HIPAA. If the patient gives us a statement of denial, determine whether our dental practice should write a rebuttal (and if so, consult with FSU General Counsel to assist with the rebuttal).

Future disclosures of the information. If the patient gives us a statement of denial, ensure that every time our dental practice discloses the information in question, we include the request for amendment, our denial, the statement of disagreement, and our rebuttal (if any) or an accurate summary of these documents.
If the patient does not give us a statement of denial, but the patient asks for our dental practice to include the request for amendment and our denial whenever our dental practices discloses the information in question, ensure that copies of these documents (or an accurate summary) is included in all such disclosures.

If the dental practice is making an electronic standard transaction that does not permit the additional material to be included, transmit the material separately.

Documentation. Document all requests for amendment and log all requests for amendment and their disposition. Retain the documentation for at least six (6) years from the date of its creation, or from the date last in effect, whichever is later.

(See Request for Amendment form, Denial of Request to Amend form, Amendment Request Log in Appendix, pages 119, 120, & 121)
ACCOUNTING OF DISCLOSURES 45 CFR 164.528 (XIV CONTINUED)

POLICY:

Upon request, our dental practice will provide a patient with an appropriate accounting of disclosures.

PROCEDURE:

Staff Duties – Every patient has the right to ask our dental practice for an “accounting of disclosures” of the patient’s information.

Immediately report to the Privacy Officer any disclosures of patient information that are not for purposes of treatment, payment or healthcare operations. Tell the Privacy Officer the date of the disclosure, who received the patient information, the information that was disclosed, and the purpose of the disclosure.

The Privacy Officer is responsible for receiving and processing all requests for an accounting of disclosures. If a patient asks you for an accounting of disclosures, politely tell them that our Privacy Official handles these requests, give them a copy of your request form, and ask them to complete the form. Give it to the Privacy Official.

Privacy Officer – Use the Log of Disclosures of Patient Information form to record all disclosures of patient information that would need to be included if a patient asks for an accounting of disclosures. Since an accounting of disclosures must include disclosures made up to six (6) years before the request, make sure the information about each of disclosures in the log is retained for at least six (6) years from the date of the disclosure.

If a patient asks for an accounting of disclosures, have the patient complete the Patient Request for Accounting of Disclosures form.

Within 60 days of the date that our dental practice receives the request:

- Provide the accounting of disclosures, or
- If our dental practice cannot provide the accounting within 60 day period, send the patient a letter extending the period for up to 30 days. The letter must state the reasons for the delay and the date on which we will provide the accounting. We are only entitled to one 30 day extension. Provide the accounting to the patient at the end of the extension period.

Maintain documentation of every request for an accounting of disclosures, every accounting of disclosures that our dental practice provides, and your designation as the person responsible for receiving and processing requests for accountings of disclosures for at least six (6) years from the date of the document’s creation or the date when the document was last in effect, whichever is later.

Every patient is entitled to one free accounting of disclosures in any 12 month period. Determine whether our dental practice will charge a fee for requesting additional accountings of disclosures in a 12 month period, or whether all accountings of disclosure will be provided for free. If a fee will be charged, determine the permissible, reasonable cost-based fee for providing an accounting of disclosures. If a
patient or personal representative requests an additional accounting of disclosures within a 12 month period, inform them of the fee and permit them to cancel or change the request in order to avoid or reduce the fee.

(See Log of Disclosures of Patient Information form and Request for Accounting of Disclosures in Appendix, pages 122 & 123)
CONFIDENTIAL COMMUNICATIONS 45 CFR 164.522 (b) (XIV CONTINUED)

POLICY:

Our practice will accommodate reasonable requests by patients to receive communications from our practice by an alternative means or at an alternative location.

PROCEDURE:

Staff Duties – If a patient asks our dental practice to contact him or her in a different way or at a different location, ask the patient to fill out our Confidential Communications form. Do not ask the patient to explain why he or she is making the request.

When our practice has agreed to a request for confidential communications, FLAG the patient’s record. Within Eagle Soft it will be done in the ALERT as “Confidential Communication” and on a paper chart it will be flagged with a colored sticker on the inside of the patient’s chart, above the patient Medical Alerts sticker.

If you are communicating with a patient whose record is flagged, make sure to abide by the Confidential Communications request. The signed Confidential Communication form is to be stored in the patient’s chart on the right hand side of the dental chart, above the signed HIPAA Consent form.

Privacy Officer – Train staff to use the Confidential Communications form when appropriate. Develop the system to flag a patient’s chart with this request and to continue to update the flagging protocol as changes are made to the dental chart.

The flag should not indicate to anyone other than our workforce that the patient has requested confidential communications.

Retain the completed forms for at least six (6) years from the date they were completed or the date when they were last in effect, whichever is later.

(See Confidential Communications form in Appendix, page 124)
RESTRICTED DISCLOSURE 45 CFR 164.522 (a) (XIV CONTINUED)

POLICY:

Our practice allows patients to request restricted use or disclosure of their patient information. As of September 23, 2013, HIPAA requires our dental practice to agree to a request not to disclose information to a health plan about a health care item or service for payment and health care operations purposes when our dental practice has been paid for in full for the item or service by the patient or by a third party, unless the disclosure is required by law. Our dental practice is not required to agree to any other kind of request for restriction, but if we do we must abide by the restriction until it is terminated.

PROCEDURE:

Staff Duties – If a patient asks you not to use or disclose his or her information in a certain way, politely tell them that only our Privacy Officer can respond to requests for restrictions and ask them to contact our Privacy Officer.

Privacy Officer – You are responsible for responding to all requests to restrict the use or disclosure of patient information. Requests for restrictions will need to be in writing using the REQUEST FOR RESTRICTED USE OR DISCLOSURE form. All requests for restrictions need to be documented. Retain all completed documentation for at least six (6) years from the date the document was completed, or at least six (6) years from the date that the document was last in effect, whichever is later.

Health Plan Restriction. As of September 23, 2013, our practice will agree to any request not to disclose patient information about a health care item or service to a health plan (medical or dental) for purposes of carrying out payment or health care operations if the information pertains solely to a health care item or service for which our dental practice has been paid in full, unless otherwise required by law. This applies whether patient pays in full or if payment comes from another source (including another health plan).

Our dental practice will flag restricted information so a claim is not submitted to the health plan, and the health plan does not review the information during an audit.

Other restrictions. Except for the health plan restriction discussed above, our dental practice is not required to agree to a requested restriction. Generally, our dental practice will agree to restrictions only in exceptional circumstances, and when our dental practice can reasonably accommodate them. Determine whether or not we should agree to each request.

If we agree to a restriction, we must not violate the restriction; however, we may use and disclose restricted information in certain situations, such as an emergency treatment, HHS investigation, and public health reporting as permitted by HIPAA.

If we agree to a restriction, the agreement can only be terminated in three ways:

1. The patient requests the termination in writing.
2. The patient orally agrees to the termination and our dental practice documents the oral agreement.

3. Our dental practice informs the patient that we are terminating our agreement to a restriction (however, our dental practice cannot terminate health plan restrictions where our dental practice has been paid in full – see above). The termination only applies to patient information that our dental practice created or received after we informed the patient that the restriction has terminated.

(See Restricted Use or Disclosure form in Appendix, page 125)
XV. TRAINING 45 CFR 164.530 (B)

POLICY:

Our dental practice will train all workforce members within a reasonable period of time after they join the practice to comply with the HIPAA policies and procedures that affect their jobs. When there is a material change to our policies and procedures, our dental practice will train the workforce members whose jobs are affected by the change within a reasonable time after the change becomes effective.

PROCEDURES:

Staff Duties – You must be trained to comply with HIPAA when you do your job. All training must be documented. When there is a significant change to our HIPAA policies and procedures that affect your job, you will receive a training update.

Privacy Officer Duties – You are responsible for making sure that each of our workforce members get the HIPAA training they need to do their jobs, including training updates when there is a change in our HIPAA policies and procedures. You must make sure that new workforce members get HIPAA training within a reasonable amount of time after joining the dental practice. When we change our policies and procedures, make sure that the workforce members affected by the change get training within a reasonable time after we put the change into effect.

You must document all HIPAA training, even on the spot refreshers. Keep the training documentation for at least six (6) years from the date the document was created or from the date when the document was last in effect. Whichever is later.

In some cases, retraining may be an appropriate sanction for workforce members who violate any one of our HIPAA policies and procedures. When retraining is used as a sanction, make sure a copy of the training documentation is placed in the person’s personnel file.

(See HIPAA Training Sign In Sheet in Appendix, page 127)
XVI. DISCIPLINARY ACTION ("Sanctions") 45 CFR 164.530 (e)

POLICY:
Our dental practice will have and apply appropriate sanctions against workforce members who violate our HIPAA privacy, security and breach notification privacy policies and procedures. Our dental practice will document all sanctions that are applied.

PROCEDURE:

Staff Duties – Our dental practice applies appropriate sanctions against workforce members who violate our HIPAA privacy, security and breach notification policies and procedures.

Privacy Officer Duties – Once a violation has been discovered, appropriate sanctions must apply. Each time a sanction is applied, you will document the sanction and retain the documentation for six (6) years from the date the document was created or from the date when the document was last in effect, whichever is later.

The individuals involved in determining the appropriate sanctions may be lead course instructors, administrators, DH Clinic Operations Supervisor, DH Clinic Facilities Coordinator, DH Clinic Clerk(s), General Counsel and/or other consultants.

Whistleblowers. Sanctions must not be imposed against whistleblowers whose actions are appropriate under the HIPAA Privacy Rule. Sanctions must not be used as a means of retaliation or intimidation in violation of HIPAA.

Intimidation and retaliation. The dental practice may not use sanctions as a means of intimidation or retaliation against a workforce member who:

• Files a HIPAA complaint with the government

• Cooperates with a government HIPAA investigation or proceeding, or

• Opposes any activity at the dental office that the workforce member believes is unlawful under HIPAA, as long as
  o The workforce member’s belief is reasonable and in good faith
  o The workforce member opposes the activity in a reasonable way and does not impermissibly use or disclose patient information

Sanctions from FSU Human Resources are as follows:

The Privacy Rules require FSU to have and apply appropriate discipline to employees who fail to comply with the Policies and Procedures or the Privacy Rules. FSU’s policy is to appropriately discipline any employee who violates the Policies and Procedures or the Privacy Rules.
**Type of Discipline.** FSU will appropriately discipline employees who fail to comply with the Policies and Procedures or the Privacy Rules, in accordance with the disciplinary policies set forth in FSU’s employee handbook, FSU’s policies and procedures, and Collective Bargaining Agreements. Discipline will vary depending on the nature of the employee’s misconduct, but discipline includes sanctions up to and including termination of employment.

**Whistleblowers.** FSU will not discipline employees who disclose PHI, so long as:

- the employee believes in good faith that the Health Plan or FSU has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Health Plan or FSU potentially endangers one or more patients, workers, or the public; and
- the disclosure was made to the individuals or agencies and for the purposes set forth in the whistleblower provisions of the Privacy Rules (see section 164.502 of the Privacy Rules).

**Crime Victims.** FSU will not discipline an employee who is a crime victim and discloses PHI to a law enforcement official, so long as the PHI concerns the suspected perpetrator of the criminal act and the PHI is limited as required by the Privacy Rules (see 45 CFR 164.502(j)).

**No Intimidating or Retaliatory Acts**

The Privacy Rules prohibit FSU from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against individuals for exercising their rights under the Privacy Rules. FSU’s policy is that FSU will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their privacy rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Rules.
XVII. RETALIATION AND INTIMIDATION 45 CFR 164.530 (g) & 45 CFR 160.316

POLICY:

Our dental practice (also applies to our business associates) will not intimidate, threaten, coerce, or discriminate against any person, nor take any retaliatory action against anyone, because he or she:

- Exercises a HIPAA right
- Participates in a process provided for by the Privacy Rule or Breach Notification Rule
- Files a complaint with the dental practice or with the Secretary of HHS concerning the HIPAA compliance of the dental practice or a business associate
- Testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing
- Opposes an act that HIPAA makes unlawful, as long as the person has a good faith belief that the act is unlawful, and the way the person opposes the act is reasonable and does not involve disclosing patient information in violation of HIPAA.

PROCEDURE:

Staff Duties — Our dental practice (also applies to our business associates) will not intimidate, threaten, coerce, or discriminate against any person, nor take any retaliatory action against anyone, because he or she:

- Exercises a HIPAA right
- Participates in a process provided for by the Privacy Rule or Breach Notification Rule
- Files a complaint with the dental practice or with the Secretary of HHS concerning the HIPAA compliance of the dental practice or a business associate
- Testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing
- Opposes an act that HIPAA makes unlawful, as long as the person has a good faith belief that the act is unlawful, and the way the person opposes the act is reasonable and does not involve disclosing patient information in violation of HIPAA.

Immediately report to the Privacy Officer if you believe or suspect that anyone at our dental practice or at one of our business associates has intimidated or retaliated against you or anyone else.
**Privacy Officer Duties** – If it is discovered that anyone at our dental practice or at one of our business associates has intimidated or retaliated against someone in violation of this policy, ensure that the intimidation or retaliation stops. See that appropriate sanctions are applied against any workforce member responsible for the intimidation or retaliation, and document the sanctions.

If a business associate engages in impermissible intimidation or retaliation in violation of HIPAA, take reasonable steps to end the violation by the business associate. If the attempt to end the violation is not successful, the dental practice must terminate the business associate agreement when possible.
XVIII. **WAIVER OF HIPAA RIGHTS 45 CFR. 530 (h) & 45 CFR 160.306**

**POLICY:**

Our dental practice will not require anyone to waive their right to complain to HHS if they believe our dental practice or another HIPAA covered entity is not complying with HIPAA, or any other rights that they have under the Privacy or Breach Notification Rule, as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

**PROCEDURE:**

**Staff Duties** – Do not ask patients to waive a HIPAA right as a condition of treatment, payment, or health plan enrollment or eligibility for benefits.

**Privacy Officer Duties** – Train all workforce members to understand that they may not require or request a patient or other person to waive:

- Any right under the Privacy Rule or Breach Notification Rule, or
- Their right to file a complaint with HHS

as a condition for the provision of treatment, payment, enrollment, in a health plan, or eligibility for benefits.
XIX. DOCUMENTATION OF HIPAA COMPLIANCE 45 CFR 164.530 (j) & 45 CFR 160.310

POLICY:

Our dental practice will maintain the following documentation as required by HIPAA:

- HIPAA privacy and breach notification policies and procedures
- Communications required to be in writing
- Documentation of actions, activities, and designations required to be documented

Our dental practice will retain this documentation for a period of at least six (6) years after its creation or last effective date, whichever is later

PROCEDURE:

Staff Duties – Do NOT dispose of, delete, or destroy any electronic or paper HIPAA document for six (6) years from the date the document was created, or six (6) years after it was last in effect, whichever is later. Examples of HIPAA documents include policies and procedures, Notices of Privacy Practices, acknowledgement forms, authorization forms, breach notification documents, etc.

Privacy Officer Duties – Maintain an electronic and/or hard copy file of our HIPAA compliance documentation.

Our HIPAA compliance documentation includes a variety of documents. Here are some examples of HIPAA compliance documentation:

- Current and past designation of the Privacy Officer
- Policies and Procedures
- Notices of Privacy Practices
- Business Associate Agreements
- Signed Acknowledgments of Receipt of Notice of Privacy Practices
- Training Sign in Sheets
- Signed Authorization forms
- Complaints about our privacy practices
- Documentation of disciplinary actions (“sanctions”) 
- Restricted Disclosures
• Disclosure logs
• Lists of Designated Record Sets
• Minimum Necessary Restrictions
• Breach Notification letters
• Logs of breaches involving fewer than 500 patients

Our HIPAA documentation must contain current versions of documents such as policies and procedures, Notices of Privacy Practices, and personnel designations. Our HIPAA documentation must also contain any prior versions of those documents unless at least six (6) years has passed since the document was created or since the document was last in effect, whichever is later. Ensure that all required HIPAA documentation is not disposed of, or deleted, destroyed, or lost for at least six (6) years from the date of its creation or the date when last in effect, whichever is later.

Dispose of HIPAA compliance documentation when it is appropriate to do so. If a document identifies or could be used to identify a patient, dispose of the document in a way that “secures” the document under the Breach Notification Rule. Hard copy documents should be shredded or destroyed such that the patient information cannot be read or otherwise reconstructed. Electronic media containing patient information should be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the patient information cannot be retrieved.
SAFEGUARD PATIENT INFORMATION 45 164.530 (c) (Administrative, Physical, and Technical)

POLICY:

(There are three categories of safeguards: administrative, physical and technical)

Staff and DH Student Duties - UNDER ALL CATEGORIES, PERSONAL PAGERS, CELL PHONES, PORTABLE COMPUTING DEVICES, AND/OR THEIR CAMERAS/VIDEOCAMERAS, PERSONAL COMPUTERS, PDA’S, BLACKBERRY’S, OR ANY OTHER PERSONAL ELECTRONIC EQUIPMENT IS NOT PERMITTED ON THE CLINIC FLOOR AND ARE PROHIBITED IN PATIENT TREATMENT LABS, CLINICAL SETTINGS AND THE DH COMPUTER LAB!

AUTHORIZED USERS: THERE ARE FEW INDIVIDUALS THAT MUST USE A CELL PHONE TO DO THEIR JOBS WHEN TROUBLE SHOOTING CLINICAL PROBLEMS; THOSE AUTHORIZED INDIVIDUALS WOULD BE: I.T. STAFF, DH CLINIC OPERATIONS SUPERVISOR, DH RADIOLOGY INSTRUCTOR, SUPERVISING DENTISTS, etc.

If a DH student needs to make a phone call to find a patient, etc., they may use the clinic land line telephone or excuse themselves from clinic, go to their locker and have the conversation with potential patients at the west end of the Health Professions building and away from the dental hygiene clinic. This safeguard will be strictly enforced. Professionalism Points may be deducted from a student’s lab or clinical grade if a violation should occur.

Work Study students that are working in the reception office area, the sterilization area are NOT authorized cell phone users and may not bring their cell phones or other electronic devices into the dental reception, clinical area. Violation of this safeguard will be strictly enforced and could result in termination.

Sharing any patient information in any form on social media such as Facebook, etc., is strictly prohibited.

Other sanctions will be determined by the Privacy Officer depending on the severity of the violation and will involve meeting with the Privacy Officer for further HIPAA training. If the violation is severe, further sanctions may involve the Department Head and/or FSU General Counsel.

ADMINISTRATIVE SAFEGUARD POLICY:

POLICY:

Our dental practice will have in place appropriate administrative, technical and physical safeguards to protect the privacy of patient information. Our dental practice will reasonably safeguard patient information from intentional or unintentional use and disclosure in violation of HIPAA. Our dental practice will reasonably safeguard patient information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure of patient information.

PROCEDURE:

Safeguards we currently have in place are as follows:
Staff and DH Student Duties - UNDER ALL CATEGORIES, PERSONAL PAGERS, CELL PHONES, PORTABLE COMPUTING DEVICES, AND/OR THEIR CAMERAS/VIDEOCAMERAS, PERSONAL COMPUTERS, PDA’S, BLACKBERRY’S, OR ANY OTHER PERSONAL ELECTRONIC EQUIPMENT IS NOT PERMITTED ON THE CLINIC FLOOR AND ARE PROHIBITED IN PATIENT TREATMENT LABS, CLINICAL SETTINGS AND THE DH COMPUTER LAB!

AUTHORIZED USERS: THERE ARE FEW INDIVIDUALS THAT MUST USE A CELL PHONE TO DO THEIR JOBS WHEN TROUBLE SHOOTING CLINICAL PROBLEMS; THOSE AUTHORIZED INDIVIDUALS WOULD BE: I.T. STAFF, DH CLINIC OPERATIONS SUPERVISOR, DH RADIOLOGY INSTRUCTOR, SUPERVISING DENTISTS, etc.

If a DH student needs to make a phone call to find a patient, etc., they may use the clinic land line telephone or excuse themselves from clinic, go to their locker and have the conversation with potential patients at the west end of the Health Professions building and away from the dental hygiene clinic. This safeguard will be strictly enforced. Professionalism Points may be deducted from a student’s lab or clinical grade if a violation should occur.

Work Study students that are working in the reception office area, the sterilization area are NOT authorized cell phone users and may not bring their cell phones or other electronic devices into the dental reception, clinical area. Violation of this safeguard will be strictly enforced and could result in termination.

Sharing any patient information in any form on social media such as Facebook, etc., is strictly prohibited.

Other sanctions will be determined by the Privacy Officer depending on the severity of the violation and will involve meeting with the Privacy Officer for further HIPAA training. If the violation is severe, further sanctions may involve the Department Head and/or FSU General Counsel.

HIPAA Training: All students and staff will be trained regarding HIPAA Policies and Procedures for this dental clinic at least annually. HIPAA will also be placed on the agenda as a permanent topic of discussion at both the Departmental meetings and Programmatic meetings.

Patient Registration: After a patient has registered, call the patient from the waiting room by first name only. After the patient has retrieved, address the patient appropriately and respectfully with Mr., Mrs., etc.

Oral Communications: speak quietly when discussing a patient’s condition in a waiting room or other area where others may hear the conversation. Avoid using names in hallways, elevators, student lounge, bathrooms, any location that is considered “public”.

Avoid unnecessary disclosures of patient information by monitoring voice levels and being alert for unauthorized listeners. Conduct telephone conversations away from public areas. Use speaker phones only in private areas.

Telephone Messages: Unless a patient has asked not to be contacted by telephone, telephone messages and appointment reminders may be left on answering machines and voicemail systems, but LIMIT the amount of information disclosed in a telephone message.
**Faxes:** Fax machines MUST be located in secure areas that cannot be easily accessed by visitors or patients.

**Mail:** Send mail to the patient’s primary address unless the patient requests an alternative address. Postcards may be used for appointment reminders as long as the patient has not objected and the postcard contains the MINIMUM NECESSARY amount of patient information.

**Copies:** Copies of records containing patient information will be stamped “copy” in a color other than black so that copies can be distinguished from originals. Traditional x-rays that have been duplicated will be marked “duplicate” on the mount along with the patient name and original date of service.

**Photocopiers, Scanners and Printers:** Some printers, scanners and photocopiers have a built in hard drives. Before our dental practice gets rid of an old or non-working piece of equipment, we will have the hard drive securely wiped by FSU IT department to prevent unauthorized individuals from accessing any patient information and other sensitive information that may be stored on the hard drive.

If the piece of equipment is leased, we will try to secure leased equipment that has a function to securely wipe the hard drives and will work with our IT staff to ensure that this function has been used to wipe the drive before returning to the leasing agency. Currently, we do not lease any of the equipment mentioned here.

**Destruction of Protected Health Information:** When it is appropriate to destroy patient information in compliance with applicable federal and state laws and our practice’s document retention policies, the information will be destroyed in a way that “secures” it under the breach notification rule.

The Privacy Officer, along with the FLITE University Archivist, IT Security Team, and others that deal with security and destruction of documents, will determine when patient information may be disposed of, who may destroy the information, and any safety precautions that apply. This will be in accordance with federal and state laws.

**Academic/clinical records with any identifiable patient information** on any portion of a student/patient form that a student is preparing prior to a patient arriving for their appointment MUST be placed in the approved shredder box if an error is made to the INITIAL paperwork prior to a patient being seen. If a student should make an error to existing paperwork that is actually a part of the patient record, draw one line through the error, initial the error and record the correct information.

Clinical paperwork DOES NOT GO INTO THE TRASH. This applies only when a student is creating a new patient chart and has made an error prior to actually seeing the patient for the first time. Dispose of in the shredder boxes located in VFS 201, 202, and 204.

The Privacy Officer will ensure that a **business associate agreement** is in place before our dental practice gives any patient information to a recycling or disposal firm. This includes companies that recycle dental x-rays.

**Verify** the identity of the vendor’s representative before turning over any patient information or devices containing patient information unless you know the representative by sight.
PHYSICAL SAFEGUARD PROCEDURES:

POLICY:

Staff and DH Student Duties - UNDER ALL CATEGORIES, PERSONAL PAGERS, CELL PHONES, PORTABLE COMPUTING DEVICES, AND/OR THEIR CAMERAS/VIDEOCAMERAS, PERSONAL COMPUTERS, PDA’S, BLACKBERRY’S, OR ANY OTHER PERSONAL ELECTRONIC EQUIPMENT IS NOT PERMITTED ON THE CLINIC FLOOR AND ARE PROHIBITED IN PATIENT TREATMENT LABS, CLINICAL SETTINGS AND THE DH COMPUTER LAB!

AUTHORIZED USERS: THERE ARE FEW INDIVIDUALS THAT MUST USE A CELL PHONE TO DO THEIR JOBS WHEN TROUBLE SHOOTING CLINICAL PROBLEMS; THOSE AUTHORIZED INDIVIDUALS WOULD BE: I.T. STAFF, DH CLINIC OPERATIONS SUPERVISOR, DH RADIOLOGY INSTRUCTOR, SUPERVISING DENTISTS, etc.

If a DH student needs to make a phone call to find a patient, etc., they may use the clinic land line telephone or excuse themselves from clinic, go to their locker and have the conversation with potential patients at the west end of the Health Professions building and away from the dental hygiene clinic. This safeguard will be strictly enforced. Professionalism Points may be deducted from a student’s lab or clinical grade if a violation should occur.

Work Study students that are working in the reception office area, the sterilization area are NOT authorized cell phone users and may not bring their cell phones or other electronic devices into the dental reception, clinical area. Violation of this safeguard will be strictly enforced and could result in termination.

Sharing any patient information in any form on social media such as Facebook, etc., is strictly prohibited.

Other sanctions will be determined by the Privacy Officer depending on the severity of the violation and will involve meeting with the Privacy Officer for further HIPAA training. If the violation is severe, further sanctions may involve the Department Head and/or FSU General Counsel.

Other safeguards we currently have in place are as follows:

Paper Records: Our dental practice will store paper records and dental charts away from unauthorized persons. Dental records will be placed face down on desks, counters and workstations to conceal the identity of the patient.

Students are to store the dental chart above the x-ray viewing box, faced into the cabinet or wall to conceal the identity of the patient.

The Clinic Clerk(s) will pull (or delegate this duty to a trained work study student specifically trained in the dental reception office) patient dental records prior to the patient visit and is responsible for ensuring that the records are safely returned to the dental records files and locked up when not in use.

Patient records may NOT be removed from the FSU Dental Hygiene Clinic and are NOT to go beyond the area of the dental clinics (VFS 201, 202, 203, 204 or 205) with the exception of those being stored in
locked file cabinets in VFS 205. Clinic Clerks and those working in the reception office are the only individuals that have access to these locked files.

All (paper) dental records must be securely returned, stored, and locked up when the dental office is closed.

Student Patient Tracking records: It has been recommended by FSU General Counsel that all student patient tracking records not be allowed to leave the clinical site, but be stored in a secure manner. As of this date, Student Performance forms (grade sheets) will have the patient name and the date of service “blackened out” professionally on their form through the FSU Copy Center and will be in the student manual for their use. When a patient is completed, the NCR copy (yellow) will go to the student with no identifiable information on it and the dental office will retain the NCR (white) copy. These forms will remain in the student’s academic file 1 year from the date the student graduates and will be shredded at that time.

DENTAL HYGIENE STUDENTS MAY ONLY USE (PAPER) DENTAL RECORDS IN VFS 201, 202, 203, OR 204

Special permission may be given to students (by the Privacy Officer and the NERB Coordinator) to use the dental charts in a pre-designated room while preparing the dental chart for the student’s NERB exam. This room may be a classroom, however, it will be a mutually agreed upon room for NERB Orientation. The NERB Coordinator will take responsibility for the security and protection of the patient’s health information and the security of the patient’s dental charts following NERB Orientation. The dental records must be securely returned to the dental records files and locked up.

Patients and Visitors: Visitors and patients will be appropriately monitored during visits to our dental practice. Patients will not be allowed to access other patient’s records or other patient information.

Authorized Access Areas: VFS 202 and VFS 205 have been signed with “Authorized Access” signs. DH students may not access these areas unless invited. All patients and/or visitors DO NOT have access to these areas. This will be strictly enforced. Each computer is labeled with a sign stating “Authorized Users Only/No Internet Access”.
**TECHNICAL SAFEGUARD PROCEDURES:** Under our current FSU computer systems, these safeguards are not fully accomplished. The Privacy Officer and the I.T. Security Officers continue to work on full compliance, however, we are not there as of this writing. Items needing further compliance are noted with an asterisk (*).

As recommended by Norbert Kugele (from Warner, Norcross, and Judd, Attorneys At Law), FSU Dental Hygiene was advised to put a statement in the Informed Consent that patients sign. The statement is as follows:

“I agree that Ferris State University Dental Hygiene clinic may send my radiographs in an electronic format and at my request will send them to the email address provided by the dentist of my choice. I am aware that there is some level of risk that third parties might be able to read unencrypted emails.”

(See Patient Bill of Rights/informed Consent in Appendix, page 129)

**POLICY:**

**Staff and DH Student Duties - UNDER ALL CATEGORIES, PERSONAL PAGERS, CELL PHONES, PORTABLE COMPUTING DEVICES, AND/OR THEIR CAMERAS/VIDEOCAMERAS, PERSONAL COMPUTERS, PDA’S, BLACKBERRY’S, OR ANY OTHER PERSONAL ELECTRONIC EQUIPMENT IS NOT PERMITTED ON THE CLINIC FLOOR AND ARE PROHIBITED IN PATIENT TREATMENT LABS, CLINICAL SETTINGS AND THE DH COMPUTER LAB!**

**AUTHORIZED USERS:** THERE ARE FEW INDIVIDUALS THAT MUST USE A CELL PHONE TO DO THEIR JOBS WHEN TROUBLE SHOOTING CLINICAL PROBLEMS; THOSE AUTHORIZED INDIVIDUALS WOULD BE: I.T. STAFF, DH CLINIC OPERATIONS SUPERVISOR, DH RADIOLOGY INSTRUCTOR, **SUPERVISING DENTISTS**, etc.

If a DH student needs to make a phone call to find a patient, etc., they may use the clinic land line telephone or excuse themselves from clinic, go to their locker and have the conversation with potential patients at the west end of the Health Professions building and away from the dental hygiene clinic. This safeguard will be strictly enforced. Professionalism Points may be deducted from a student’s lab or clinical grade if a violation should occur.

Work Study students that are working in the reception office area, the sterilization area are NOT authorized cell phone users and may not bring their cell phones or other electronic devices into the dental reception, clinical area. Violation of this safeguard will be strictly enforced and could result in termination.

Sharing any patient information in any form on social media such as Facebook, etc., is strictly prohibited.

Other sanctions will be determined by the Privacy Officer depending on the severity of the violation and will involve meeting with the Privacy Officer for further HIPAA training. If the violation is severe, further sanctions may involve the Department Head and/or FSU General Counsel.
The Dental Hygiene Privacy and Security Policies and Procedures is a working document and as updates to our electronic equipment and FSU email systems update, etc., occurs, it is our intent to update our policies and procedures on an annual basis.

*Encryption:* Electronic patient information should be encrypted whenever the Security Official determines that it is reasonable and appropriate to do so. Our dental practice will consult with our software vendor and internet provider to determine encryption solutions that would render patient information “secure” under the Breach Notification Rule. Emails sent between our dental practice and other health care providers via a common Internet carrier shall not include patient information unless the email is encrypted.

*Internet:* Unauthorized access to the Internet from a computer workstation that contains patient information is prohibited.

Our dental practice encourages staff to use their personal electronic devices to check personal emails or conduct personal Internet business away from the dental clinic.

**Portable and Mobile Handheld Computing Devices:** DH Students and workforce members may **NOT** store patient information on portable or mobile computing devices.

DH Students and workforce members who store any unsecured patient information on portable or mobile handheld computing devices are responsible for the security of the patient information and are subject to sanctions up to and including termination of school or employment if the device is misplaced, lost or stolen. DH Students and workforce members must IMMEDIATELY notify the Privacy Officer of a breach or suspected breach of protected health information.

**Portable Storage Devices:** Patient information **MAY NOT** be downloaded onto portable storage devices, such as USB devices and CD-ROMs UNLESS its purpose is to provide a patient requested information. All patient requested downloads must be in writing. A patient receiving an electronic copy of patient information may request the copy unencrypted on a portable storage device, and our dental practice will provide the copy in that format if requested and if we can readily produce it.

**Clinic Computers:** All computers storing patient information must be turned off when clinic is not in session with the exception of the dental office computers. Office clinic clerks will need to use the software system even while patient treatment clinics are not in session for patient scheduling, patient cancellations, various financial reports, etc.

All clinic computers, with the exception of the teacher station in VFS 201 are to be used for clinical applications and treatment of patients, only.
Access Authorization/Password Security: All individuals must log in to all clinic computers using their own username and password as recommended by FSU I.T. Data Security Administrator. The FSU Password Security Statement is as follows:

FSU Password Security Statement
Lori Henderson, Data Security Administrator
Data Security Office

Please Keep Your ID and Password Secure

Ferris State University is a single sign-on/consistent sign-on environment making it more efficient to access our information. The caution that goes along with this is that you must be diligent about protection of your information and the personal information of others. This means you are the only one to use your User ID and password.

Please be aware that the Confidential Data Security Agreement form indicates in the second bullet that, “any user ID and/or password issued for my exclusive use is not be shared with or delegated to others, and I am responsible for the security of the same.” The last paragraph of the form states that, “I understand that failure to abide by this agreement will result in my data access being discontinued and/or disciplinary action, with the possibility of termination of employment at Ferris State University, and may subject me to further civil or criminal sanctions.” The complete form can be viewed on MyFSU under the Workplace tab, University Forms section.

The seriousness of sharing an ID is compounded by access that a student worker or co-worker with inappropriate access could have to information across the campus, such as making class section changes, registering students into any offered section, adding charges to any student and viewing financial aid information. They could also potentially enter Direct Pay checks, view personal information such as salaries, home addresses, and phone numbers. In addition, when someone’s ID and password are shared, their own personal information can be viewed on MyFSU, such as pay stubs, vacation time, sick time, beneficiaries and dependents’ social security information, retirement plans, w4 allowances, etc.

Please be aware that there are options for student workers as well as access to employees covering temporary job duties. Employees who have access to University information need to be aware of their responsibility to keep their ID’s secure. If you have any questions regarding your access, please contact the Data Security Office via email at DataSecurity@ferris.edu.

Access Authorization/Password Security within EagleSoft: All users are given access to the EagleSoft according to their job description or if they are a dental hygiene student. All dental hygiene students will have minimal access within EagleSoft to minimize any risk of access record deletion, etc. Most of the student access is view only, with the exception of dental x-rays, periodontal charting, and hard tissue charting.
XXI. **DE-IDENTIFICATION 45 CFR 164.502 (d) (2)**

**POLICY:**

Our dental practice will properly de-identify patient information when appropriate.

**PROCEDURES:**

**Staff Duties** – De-identifying patient information involves removing very specific information that can be used to identify a patient. Staff members who have not been trained to de-identify patient information should not attempt to do so or be assigned to do so.

**Use the following method to “de-identify” patient information**

Remove from the document all of the following “identifiers” for the patient and for the patient’s relatives, household member, and employers:

1. Names, including initials
2. Any geographic subdivision smaller than a state (including address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, - the geographic unit formed by combining all zip codes with the same three digits must contain more than 20,000 people; otherwise, the three digit code must be changed to “000”,)
3. All elements of dates (except year) for dates directly related to the individual, including birth date, treatment date, lab work date, date of death; all ages over 89 and all elements of dates (including year) that indicate an age over 89
4. Telephone numbers
5. Fax numbers
6. Electronic email addresses
7. Social security numbers, including the last four digits
8. Medical/dental chart or record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

The information is not considered de-identified if our dental practice (FSU Dental Hygiene clinic) has any actual knowledge that the information could be used. This applies to information that could be used alone or in combination with any other information to identify an individual who is the subject of the information.
Avoid using redaction to de-identify a document

Remove the identifiers using a method that makes it impossible to read or re-create the identifiers, whether the document being de-identified is in hard copy or electronic format.

DO NOT use a pencil, pen, marker, etc., to hide the 18 identifiers on a paper document. This is because sometimes “redacted” information can still be read, especially if the document is photocopied or scanned. This can lead to a HIPAA violation or breach. Redaction cannot be used as a method of securing patient information under the BREACH NOTIFICATION RULE.

FOR MORE INFORMATION ON THIS RULE GO TO:


Privacy Officer Duties – Educate and train staff. HIPAA does not apply to PROPERLY de-identified patient information. Using and disclosing properly de-identified patient information when appropriate may help our dental practice avoid HIPAA violations and breaches of unsecured patient information. For example, if an instructor for a course would like to use a patient as a case study, providing the patient records with properly de-identified information can minimize the likelihood of breach. Additionally, if the only information we provide is properly de-identified, then HIPAA rules no longer apply.
XXII. BREACH NOTIFICATION 45 CFR 164.400 & 45 CFR 164.414

POLICY:

When our dental practice or one of our business associates discovers a possible breach of unsecured patient information, our dental practice will investigate and provide timely notification in compliance with HIPAA and applicable state laws, unless our dental practice can demonstrate, through an appropriate assessment of the relevant factors, including the four required factors, that there is a low probability that the information has been compromised.

PROCEDURES:

Staff Duties – Be alert for possible breaches and notify the Privacy Officer immediately if you suspect a breach has occurred. Following our dental practice’s Privacy and Security Policies and Procedures can help minimize possible breaches of unsecured patient information.

Privacy Officer Duties – Put Breach Notification as defined by FSU General Counsel into action. Update the policies and procedures when appropriate, such as when there is a change in the law. Train workforce members to comply with the policies and procedures. In particular, train workforce members to notify the Privacy Officer immediately if they even suspect that a breach of unsecured patient information may have occurred. Train staff to follow our dental practice’s Privacy and Security Policies and Procedures to minimize possible breaches of unsecured patient information.

Investigating and assessing possible breaches. If a breach is discovered, or if a workforce member or business or a business associate tells you about a possible breach, investigate immediately. If a breach of unsecured patient information has occurred, our dental practice may choose to provide the required notifications without performing a risk assessment. However, notification is not required if our dental practice can demonstrate that there is a low probability that the information has been compromised, based on an analysis of the relevant factors, including the four factors required under the Breach Notification Rule. Document the analysis using our Breach Assessment form. (See Breach Notification form in Appendix).

Sending Notification. If notification is required, consult with FSU General Counsel and, if necessary, draft notice letters that comply with HIPAA and other applicable law, and provide timely notice (complying with any applicable law enforcement delay) to affected individuals, HHS, and if required, to the media. Breaches involving 500 or more individuals must report to FSU General Counsel, who then will determine what to report to HHS without unreasonable delay. The breach must be reported no later than 60 days after the discovery of the breach.

A log must be maintained of all breaches involving fewer than 500 individuals and submit the log annually to FSU General Counsel to be submitted to HHS.

Substitute Notice. If we lack contact information for nine or fewer individuals involved in a breach, consult with FSU General Counsel and proceed to contact the individuals via phone or using another means reasonable calculated to reach them. Do not provide patient information to unauthorized persons when providing substitute notice.
If we lack contact information for 10 or more individuals affected by a breach, consult FSU General Counsel to determine whether to post a conspicuous notice about the breach on the homepage of our website for 90 days, or to provide a conspicuous notice in major print or broadcast media in the area where the affected individuals likely reside, then provide substitute notice. Either form of notice must direct individuals to a toll-free telephone number that is active for at least 90 days that people can call to find out if their information was involved in a breach.

**Electronic Communications.** Determine whether asking patients to sign agreements permitting electronic communications would help the dental practice notify patients in the event of a breach of unsecured patient information. If so, develop an agreement to receive electronic communications and develop and implement a process for requesting patient signatures and maintaining a record of the patients who have signed the agreement and an up-to-date record of the patient’s email addresses, and a record of patients who have withdrawn their agreement to receive electronic communications.

Documentation. Retain all documentation related to our dental practice’s compliance with the Breach Notification Rule for at least six (6) years from the date the document was created, or from the date the document was last in effect, whichever is later. Examples of breach notification documentation includes policies and procedures, breach assessment forms, copies of notification letters, logs, media notices, and press releases.

*(See Breach Notification form, Breach Assessment form, Breach Log, and Agreement to Receive Electronic Communication form in Appendix, pages 133, 137 & 149)*
XXIII. COMPLAINTS 45 CFR 164.530 (d), 45 CFR 164.530 (a) (1), 45 CFR 164.520 (b) (1) (vi) & 45 CFR 160.306

POLICY:

Our dental practice will provide a process for complaints about our HIPAA Privacy and Breach Notification policies, procedures, and compliance. Our practice will document any complaints received and their disposition, if any.

PROCEDURES:

Staff Duties – The Privacy Officer is responsible for receiving and processing complaints about our dental practice’s privacy practices. If anyone complains to you about the privacy of patient information at our dental practice, or about how our dental practice complies with HIPAA, immediately put the person in touch with the Privacy Official.

Privacy Officer Duties – The Privacy Officer is designated to receive complaints about the privacy of patient information at our dental practice and about how our dental practice complies with HIPAA. When anyone makes a complaint, you must:

- Receive the complaint (by listening if the complaint is oral, or by reading if the complaint is in writing)
- Enter the time, date, and a brief description of the complaint into our complaint log
- Determine the appropriate disposition of the complaint (any required follow up)
- Communicate and seek advice, if necessary, with FSU General Counsel

  o Should a sanction (disciplinary action) be applied against a workforce member who violated a policy or procedure?
  o Should an unauthorized disclosure be logged in case a patient asks for an accounting of disclosures?
  o Has there been a breach of unsecured patient information requiring notification?

Retain all documentation related to complaints for at least six (6) years from the date the document was created, or six (6) years from when the document was last in effect, whichever is the later.

At no time will our practice retaliate against an individual for filing a HIPAA complaint.

(See Complaint Log form in Appendix, page 154)
XXIV. **FUNDRAISING 45 CFR 164.514 (f) & 45 CFR 164.520 (b) (1) (iii) (A)**

**POLICY:**

Our dental practice does not conduct fundraising for the benefit of the FSU Dental Hygiene Clinic. Our dental practice will not use or disclose patient information to raise funds for the dental practice itself and will ensure that 45 CFR 164.514 (f) and 45 CFR 164.520 (b) (1) (iii) (A) are met.

**PROCEDURES:**

**Staff Duties** – Do not make fundraising requests to patients or use or disclose patient information for any purpose involving fundraising for monetary gain for the FSU Dental Hygiene Clinic.

**Privacy Officer Duties** – Train staff not to make fundraising requests to patients that would benefit the FSU Dental Hygiene Clinic, monetarily. Do not use or disclose patient information (FSU Dental Hygiene Clinic) for fundraising purposes.

Our dental practice will not use or disclose patient information to raise funds for the dental practice itself and will ensure that 45 CFR 164.514 (f) and 45 CFR 164.520 (b) (1) (iii) (A) are met and train staff to comply with the applicable procedures.

*(See Notice of Privacy Practices in Appendix, page 73)*
XXV. REVIEW AND REVISE 45 CFR 164.530 (i)

POLICY:

Our dental practice will revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA. It is recommended that a HIPAA Compliance Update Service is contracted or purchased from the American Dental Association so as the Privacy Officer and others involved in updating the FSU Dental Hygiene Clinic HIPAA Manual can remain current with federal, state, and local law.

Consultation and legal advice may need to occur with FSU General Counsel.

Staff Duties – Our dental practice will revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA. It is the staff’s responsibility to read, review, learn and know our HIPAA policies and procedures to ensure our patient’s privacy. It is also our staff’s responsibility to train, mentor, and guide our student population so that they understand the severity and consequences of their actions regarding patient privacy rights.

Faculty Duties - It is recommended that for any laboratory and clinic in our program (where patients are provided services), that each course faculty person addresses HIPAA in their course syllabus and to indicate that consequences will occur should the student not follow patient privacy practices. Penalties or sanctions should be serious enough so that students understand that they will be held accountable for their actions.

Privacy Officer – Revise our dental practice’s privacy and breach notification policies and procedures as appropriate so that our dental practice remains in compliance with HIPAA.

When our Policies and Procedures are revised, train our workforce to comply with the new policies and procedures.

If a change affects our Notice of Privacy Practices, consult with FSU General Counsel to revise the NPP as is appropriate.

Document any changes to our HIPAA policies and procedures, and retain both the new and the old policies and procedures for at least six (6) years from the date the document was created or the date when the document was last in effect, whichever is later.
ACKNOWLEDGEMENT OF RECEIPT OF HIPAA POLICIES AND PROCEDURES
(To Be Signed By All Employees/Students in the Dental Hygiene Department)

FERRIS STATE UNIVERSITY DENTAL HYGIENE CLINIC

I have received and reviewed a copy of our dental practice’s privacy, security and breach notification policies and procedures.

I understand that I should ask our dental practice’s Privacy officer if I have any questions about these policies and procedures.

Print Name: __________________________________________________________________________

Signature: __________________________________________________________________________

Date: ______________________________________________________________________________
## APPENDIX

<table>
<thead>
<tr>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer Job Description</td>
<td>69</td>
</tr>
<tr>
<td>Privacy Officer Designation</td>
<td>71</td>
</tr>
<tr>
<td>Acknowledgment of Receipt of HIPAA Policies and Procedures</td>
<td>72</td>
</tr>
<tr>
<td>Notice of Privacy Practices (NPP)</td>
<td>73</td>
</tr>
<tr>
<td>Designated Record Sets</td>
<td>80</td>
</tr>
<tr>
<td>Workforce Access to Patient Information List (Sample List)</td>
<td>82</td>
</tr>
<tr>
<td>Workforce Access to Patient Information List (Actual 2013-2014)</td>
<td>84</td>
</tr>
<tr>
<td>Routine Disclosures and Requests Form</td>
<td>90</td>
</tr>
<tr>
<td>Verification of Identity Form</td>
<td>92</td>
</tr>
<tr>
<td>Explanation of Required Disclosure (ADA Guidebook, Page 30)</td>
<td>93</td>
</tr>
<tr>
<td>Decision Tree Decedent PHI (Deceased Patient)</td>
<td>94</td>
</tr>
<tr>
<td>Authorization Form for Use and Disclosure of Patient Information Using Core Elements</td>
<td>95</td>
</tr>
<tr>
<td>Business Associate Agreement Template (use when no written agreement exists)</td>
<td>97</td>
</tr>
<tr>
<td>Business Associate Agreement Template (use when there is an existing contract)</td>
<td>107</td>
</tr>
<tr>
<td>Request for Access Form</td>
<td>117</td>
</tr>
<tr>
<td>Request for Amendment Form</td>
<td>119</td>
</tr>
<tr>
<td>Denial of Request to Amend Form</td>
<td>120</td>
</tr>
<tr>
<td>Amendment Request Log</td>
<td>121</td>
</tr>
<tr>
<td>Log of Disclosures of PHI</td>
<td>122</td>
</tr>
<tr>
<td>Request for Accounting of Disclosures Form</td>
<td>123</td>
</tr>
<tr>
<td>Confidential Communications Form</td>
<td>124</td>
</tr>
<tr>
<td>Restricted Use or Disclosure Form</td>
<td>125</td>
</tr>
<tr>
<td>HIPAA Training Sign In Sheet Template</td>
<td>127</td>
</tr>
<tr>
<td>Patient Bill of Rights and Informed Consent Form</td>
<td>129</td>
</tr>
<tr>
<td>Course Digital Camera Policy</td>
<td>130</td>
</tr>
<tr>
<td>Breach Assessment Form</td>
<td>133</td>
</tr>
<tr>
<td>Breach Notification Form</td>
<td>137</td>
</tr>
<tr>
<td>Breach Log Form (For HHS Annual Reporting)</td>
<td>149</td>
</tr>
<tr>
<td>Agreement to Receive Electronic Communication Form</td>
<td>153</td>
</tr>
<tr>
<td>Complaint Log Form</td>
<td>154</td>
</tr>
<tr>
<td>Section Notebook Protocol for DHYG 105/126</td>
<td>155</td>
</tr>
<tr>
<td>Section Notebook Protocol for DHYG 222/233</td>
<td>156</td>
</tr>
<tr>
<td>Interoffice Memorandum RE: Locked File Cabinets in VFS 202</td>
<td>157</td>
</tr>
<tr>
<td>Example of Student Performance Forms</td>
<td>158</td>
</tr>
<tr>
<td>DHYG 208 Case Study/Journal Patient Information Request Form (For De-Identification)</td>
<td>167</td>
</tr>
</tbody>
</table>
PRIVACY OFFICER JOB DESCRIPTION

GENERAL DUTIES:

Maintain the privacy of patient information and oversee activities that keep our practice in compliance with the HIPAA Privacy and Breach Notification Rule and applicable state laws on privacy, data security, and patient records.

SPECIFIC DUTIES:

The Privacy Official has the following specific duties:

- **Management Advisor**
  Work with the dental practice’s management team and lawyers to comply with applicable federal and state laws. Stay current on privacy laws and updates in privacy technology. Immediately notify the direct Administrator (Theresa Raglin) of any communication from or on behalf of governing agency, such as the Office for Civil Rights or the state attorney general, (for example, if the dental practice receives a communication about a notice of investigation, compliance review, or audit).

- **Policies and Procedures**
  Develop, or serve as a team leader in the development of, compliant privacy and breach notification policies and procedures. Implement the policies and procedures and integrate them into the practice’s day-to-day activities.

- **Training and Sanctions**
  Provide timely training (planned courses, updates, reminders, and on-the-spot refreshers) to all workforce members, including management, employees, temps trainees, volunteers, and others whose work for our academic dental hygiene practice is under the practice’s direct control. Oversee sanctions for violations of HIPAA and our privacy policies and procedures according to our policies, and bring any sanctions to the attention of the direct Administrator (Theresa Raglin).

- **Risk Management**
  Collaborate with appropriate University Security Official to ensure that privacy and security risks are analyzed, documented and updated as appropriate.
• **Business Associates**
  Ensure that appropriate agreements are in place with each of our academic dental hygiene practice’s business associates. Lead the practice in developing and updating business associate agreements and work with the committee and lawyers to develop and execute compliant business associate agreements.

• **Patient Rights**
  Respond to patient requests regarding their information and to questions about our privacy practices. Maintain documentation related to patient requests. Help the academic dental hygiene practice’s employees understand how to respond appropriately to patient questions about their information and our privacy practices.

• **Documentation**
  Create, receive, and maintain documentation related to our privacy practices, and retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. Organize documentation for prompt retrieval in the event of a government investigation or audit.

• **Complaint Management**
  Receive, respond to, and document complaints about our privacy practices, investigating complaints and mitigating harm where appropriate. Educate workforce on our policies and procedures on complaints, and that retaliation and intimidation is prohibited against individuals who exercise their patient rights.

• **Qualifications**
  Must be familiar with dental and administrative functions of the academic dental hygiene practice; have excellent communication, problem solving, and research skills and an interest in privacy laws and regulations; be recognized detail-oriented and having high integrity; have strong organizational skills and work well with management and staff.
PRIVACY OFFICER FOR THE COLLEGE OF HEALTH PROFESSIONS

Effective August 26, 2013,

Designates the Dental Hygiene Clinic Operations Supervisor as:

- The Privacy Officer, responsible for developing and implementing the dental practice’s privacy policies and procedures, and as
- The person for receiving complaints
- Providing further information about the Notice of Privacy Practices (for example, to patients, to staff, etc.), and
- Receiving and processing:
  1. Requests for access
  2. Accountings of disclosures
  3. Requests for amendments

Dental Hygiene Clinic Operations Supervisor
Ferris State University
College of Health Professions
200 Ferris Drive
Big Rapids, MI 49307

Telephone: 231-591-2260
I, _______________________________________, have received training regarding the FSU Dental Hygiene Clinic’s health information privacy policies and procedures.

I agree to comply with HIPAA privacy policies at all times and to the best of my ability. Furthermore, if I notice that there are accidental violations, I will bring the incident to the attention of the student, staff, etc., so that accidental violations do not occur.

If I notice that there are repeated violations involving one particular individual, I will bring that information to the attention of my supervisor/instructor, which will be brought to the attention of the DH Clinic Operations Supervisor immediately for correction.

Print Name: ____________________________________________________________

Signature: ______________________________________________________________

Date: ____________________________________________________________________
NOTICE OF PRIVACY PRACTICES

Effective Date of Notice: September 23, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice, please contact us at:

Dental Hygiene Clinic Operations Supervisor
Ferris State University
College of Health Professions
200 Ferris Drive
Big Rapids, MI 49307
231-591-2260

WE WILL COMPLY WITH THIS NOTICE

This Notice describes the privacy practices of Ferris State University’s Dental Hygiene Clinic, our providers, our pharmacies, and any third parties that help us manage Protected Health Information. In general, we may use and disclose your health information to coordinate and oversee your medical treatment, pay your medical claims, and assist in health care operations as described in this Notice.

OUR COMMITMENT TO PROTECT YOUR HEALTH INFORMATION

We believe that information about you and your health, whether it be in verbal, written, or electronic format is personal and should be carefully safeguarded. We are committed to protecting your personal health information. We (or the third parties that assist us) maintain a record of all health care provided by or paid for by Ferris State University. This Notice applies to all of your health information that we maintain. Please be aware that health care providers or pharmacies not associated with us, such as other doctors, dentists, hospitals, or outside pharmacies, have their own policies regarding their use and disclosure of your health information created in their offices. You should consult their Notice of Privacy Practices for information about how they may use and disclose your health information.
This Notice informs you about the ways we may use and disclose your health information. This Notice also describes your privacy rights, along with the obligations that we have regarding the use and disclosure of your health information. Federal medical privacy law requires us to:

- make sure your health information is kept private;
- give you this Notice of our Privacy Practices with respect to your health information; and
- follow the terms of this Notice.

**HOW WE MAY USE AND DISCLOSE YOUR HEALTH INFORMATION**

We do not sell your personal health information or disclose it to companies that wish to sell you their products. We must have your written permission (called an "authorization") to use and disclose your health information, except for the uses and disclosures described below. We do not sell your health information to anyone or disclose your health information to other companies who may want to sell their products to you (e.g. catalog or telemarking firms). Additionally, Michigan law may require that we obtain your specific prior authorization to use and disclose certain health information, such as behavioral health, substance abuse and HIV/AIDS information.

- **You and Your Personal Representative.** We may disclose your health information to you or your personal representative (an individual who has the legal right to act on your behalf).

- **Others Involved In Your Care.** We may share your health information with family members or friends who are directly involved in your medical care, or the payment of your medical care, when you are present and have given us verbal or written permission. We will not discuss your health information with your family or friends if you are not present unless you have given us your permission or we believe it is in your best interest. Our health professionals will exercise their professional judgment in determining when friends and family members may receive health information (e.g., a family member picking up a prescription from the pharmacy for a sick individual).

- **Treatment.** We may use your health information or disclose it to third parties to aid with your medical treatment. We may disclose health information about you to doctors, nurses, pharmacists, technicians, medical students, or other persons who are involved in taking care of you. For example, the Dental Hygiene Clinic may give your health information to your dentist for follow up services, or to a physician or other healthcare provider for oral surgery or other treatment.
• **Payment.** We may use your health information or disclose it to third parties in order to obtain payment for the services that we provide to you. For example, we may discuss your health information with your insurer to determine whether your health plan will cover the treatment.

• **Health Care Operations.** We will use and disclose your health information for general administrative and managerial functions, and activities such as quality assessment and improvement, providing educational training programs for medical, nursing, dental, and other health and non-health care professions, accreditation, certification, and licensing. Examples of how we use or disclose your health information for health care operations are: financial or billing audits; internal quality assurance; personnel decisions; participation in managed care plans; training of students, including imaging of treatment sessions; defense of legal matters; business planning; and outside storage of our records.

• **Appointment Reminders And Health Related Benefits And Services.** We may use and disclose your health information to remind you about appointments for medical care in our offices.

• **Research.** We may use or disclose your health information to third parties for research purposes when an Institutional Review Board has determined that such disclosure is appropriate without your permission.

• **Marketing.** We may also engage in face-to-face communication with you about alternative treatment options available to you, or communicate with you about the health related services available to you through the Dental Hygiene Clinic. We may also give you promotional gifts of nominal value as a method of marketing our services. Before we can use your health information for other marketing purposes or receive payment for sending marketing communications, we must first obtain your written authorization.

• **As Required By Law.** We will disclose your health information to third parties when required to do so by federal, state or local law. For example, we may share your health information when required to do so by state workers' compensation law, the Department of Health and Human Services, or state regulatory officials.

• **To Avert A Serious Threat To Health Or Safety.** We may use and disclose your health information to third parties when it is necessary to prevent a serious threat to your health and safety or to the health and safety of the public or another person. Any disclosure, however, would only be to someone able to assist in preventing the potential harm.

• **Lawsuits and Disputes.** If you are involved in a lawsuit or a dispute, we may disclose your health information in response to a court or administrative order. We may also disclose your health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only after we make efforts to inform
you of the request or to obtain an order protecting the requested information. If you are a party to a lawsuit in a Michigan court case, a court order or your authorization must be provided to release your health records (in addition to a subpoena).

- **Public Policy Matters.** We may use or disclose your health information in certain limited instances for matters involving the public welfare, such as:
  - for public health risks (e.g., prevention or control of disease, reporting births and deaths, reporting abuse and neglect) or for research purposes when there are sufficient privacy protections in place.
  - to a health oversight agency for activities authorized by law (e.g., audits, investigations, inspections, and licensure necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws)
  - to law enforcement officials (in response to a court order, subpoena, warrant, summons or similar process or to report certain kinds of crimes) and to national security officials under certain limited circumstances
  - to a funeral director, coroner, or medical examiner to permit them to carry out their duties
  - to facilitate organ donation and specified research purposes, so long as certain safety measures are in place to protect your privacy

- **Employers and Plan Sponsors.** In order for you to be enrolled in a health plan, we may share limited information with your employer or other organizations that help pay for your health coverage. However, if your employer or another organization that helps pay for your health coverage asks for specific health information, we will not share your health information unless they first obtain your written authorization.

- **Business Associates.** We hire third parties to provide us with various services that are necessary for our health plan to function. Before we share your health information with these companies, we will have a written contract with them in which they promise to protect the privacy of your health information.

- **Fundraising.** We may use and disclose your health information for fundraising communications; however, you have the right to opt out of receiving future fundraising communications.

- **Other Uses and Disclosures of PHI.** We have no plans to use or disclose your health information for purposes other than those provided for above or as otherwise permitted or required by law. If you provide us an authorization to use or disclose your health
information to third parties, you may revoke the authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information for the reasons covered by your written authorization. Please remember that we are unable to take back any disclosures we have already made with your authorization.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

You have several rights regarding your health information and we will respect your right to exercise them. If you wish to exercise your rights, you must submit a written request on a standard form we will provide to you. You can obtain this form by calling the Dental Hygiene Clinic at (231) 591-2260, or by writing to us at Dental Hygiene Clinic Supervisor, Ferris State University, College of Health Professions, 200 Ferris Drive, Big Rapids, MI 49307. The form is also available on our website, http://ferris.edu/HTMLS/colleges/alliedhe/DentalHygiene-MedicalImaging/dental-hygiene/DENTAL-NOTICES-OF-PRIVACY-PRACTICES.pdf.

- **Right To Inspect And Copy.** You have the right to inspect and copy your health information that we maintain. Usually this includes your medical and billing records. If you request a copy of the information, we may charge a fee for our costs of providing the copy. We may deny your request to inspect and copy in very limited circumstances. If we deny your request to access your health information, we will explain why the request was denied and whether you have the right to a further review of the denial.

- **Right To Request Amendments.** If you feel that your health information is incorrect or incomplete, you may ask us to correct the information. You must include with your request an explanation of how and why your health information needs to be corrected. We may deny your request for correction in certain limited circumstances. If we agree to your request for correction, we will take reasonable steps to inform others of the correction.

- **Right To Request An Accounting Of Disclosures.** You have the right to request an accounting of disclosures. This is a list of certain disclosures of your health information that we have made to third parties. This is limited to disclosures during the last three years. If you request this accounting more than once in any 12 month period, we may charge you for the cost of responding to these additional requests. Your request should tell us how you want the list (e.g., on paper, via e-mail, or on a disk).

- **Right To Request Additional Restrictions.** You have the right to request a restriction on how we use or disclose your health information to third parties for your medical treatment, payment of your medical claims, or management of our health care operations. You also have the right to request a limitation on how we disclose your health information to those involved in your care or the payment for your care, such as a family member or friend. For instance, you can request that we not disclose information to your spouse or children concerning a sensitive surgical procedure or a disease you have suffered. Please note that under federal law, we are generally not required to agree to
your request. However, if you pay the full cost of your treatment without any contribution from a health plan, your health care provider will agree upon your request not to share your treatment with your health plan for payment or health care operations purposes.

- **Right To Request Confidential Communications.** We communicate to you information about your health care treatment and payment. If you feel that our communicating with you may endanger you, you may request that we communicate with you using a reasonable alternative means or location. For example, you can ask that we contact you only at work, by e-mail, or by mail at a specified address (such as a P.O. box, rather than your home mailing address). We will accommodate all reasonable requests.

- **Right To A Paper Copy Of This Notice.** You have the right to receive a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. You may obtain a copy of this Notice on our website,


  or by writing to us at the address listed above.

- **Right to Receive Notification of a Breach of Your Health Information.** You will receive timely notification if there is a breach of your unsecured health information.

**CHANGES TO THIS NOTICE**

We have the right to change the terms of this Notice. We also have the right to make these changes apply to health information we already have about you, as well as any we receive or create in the future. We will post a copy of the most current Notice on our website,


and in our dental clinic and have a copy available for you to request and take with you. Please look at the top right-hand corner of the Notice to determine the Notice's effective date.

**QUESTIONS OR COMPLAINTS**

If you have questions about your privacy rights described in this Notice, or if you believe that we may have violated your privacy rights, please contact us at:

Dental Hygiene Clinic Operations Supervisor
Ferris State University
You may also file a written complaint with us, as well as with the Department of Health and Human Services. We support your right to protect your health information. **We will not penalize you or retaliate against you for filing a complaint.**
Designated record set means a group of records maintained by or for the dental practice that is:

a. The medical/dental records and billing records about patients maintained by or for the dental practice or

b. Used, in whole or in part, by or for the dental practice to make decisions about patients.

For the purposes of this definition, the term “record” means any item, collection, or grouping of information that includes patient information and is maintained, collected, used, or disseminated by or for the dental practice. 45 CFR § 164.501.

The following record sets are housed with Ferris State University Dental Hygiene Clinic:

1. **Eagle Soft electronic software patient records** – all persons that become a patient of Ferris State University Dental Hygiene Clinic are input into the electronic patient management software system. This information could include names, addresses, social security numbers, dates of birth and other dates relating to patient treatment, telephone numbers, dental chart numbers, health plan account numbers, etc.

   Charting components of Eagle Soft COULD include medical/dental histories, medications lists, hard tissue charts, periodontal charts, treatment care plans, x-ray and sealant information, and dates of appointments.

   Not all patients have an electronic copy of their medical/dental information because currently Eagle Soft is only used in clinic for specific assignments with students.

   Eagle Soft Software Patient Management System is networked within the Ferris State University Dental Hygiene clinic and does not have apps for Smart Phones or other electronic devices. It is a system that is password driven. This system is installed on computers in VFS 201 (Clinic), 202 (Dental Reception office), 204 (the DH Clinic Operations Supervisor’s office), and 205 (a computer room that houses 6 computers for student use only to be able to determine if they have patients or not throughout the week). This is a secured and posted room.

2. **Paper Dental Charts** – all persons that become a patient of Ferris State University Dental Hygiene Clinic have a paper dental chart made. This dental chart contains names, addresses, social security numbers, dates of birth and other dates relating to patient treatment, telephone numbers, dental chart number (which is derived from the Eagle Soft software system), health plan account numbers, Patient Consent forms, Patient Bill of Rights forms, etc.
This chart also includes a medical/dental histories, medications lists, hard tissue charts, periodontal charts, treatment care plans, plaque indices forms, immunization records, HIPAA Authorization forms, x-ray and sealant authorization forms, and services rendered forms with dates of appointments recorded.

3. **Billing records** – all patients will have a paper and electronic billing record. The billing record will have the patient’s name, chart number, the provider’s name (which is the student hygienist), and the service code and explanation and date of service along with the fee. Also included could be Medicaid numbers and Delta Dental plan ID numbers (these are only recorded in the electronic chart).

Paper billing records are stored for one semester, by the month, in VFS 202. At the end of each semester, they are removed from that file and stored in VFS 201 in a locked cabinet at the south end of clinic. All records will be stored for 6 years before they are shredded.
This form documents workforce access to patient information.

This document was created on (date):

and was in effect until ____________________________________________

<table>
<thead>
<tr>
<th>Name of workforce member</th>
<th>Patient Information Needed to do the job</th>
<th>Any conditions that apply to this access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name of workforce member</td>
<td>Patient Information Needed to do the job</td>
<td>Any conditions that apply to this access</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

WORKFORCE ACCESS TO PATIENT INFORMATION LIST

This form documents workforce access to patient information.

This document was created on: October 1, 2017

and is in effect until May 2018. or when each student’s work study grant runs out.

WORK STUDY STUDENTS IN DENTAL HYGIENE 2013-14

<table>
<thead>
<tr>
<th>Name of workforce member</th>
<th>Patient Information Needed to do the job</th>
<th>Any conditions that apply to this access</th>
</tr>
</thead>
</table>
| S. C. Office work study employee | • Work study students would need to be able to access the paper copy of the dental chart and the electronic copy of the dental chart.  
• Work study students print schedules, pull charts, file charts, audit charts for specific documentation. | • HIPAA Training  
• Patient records paper copies  
• Patient records electronic copies  
• Access to EagleSoft software is customized for each work study student based on their level of training or the number of years worked in the office.  
• Only 2 people in the DH department can customize all employee access for security reasons. |
<p>| M. K. Office work study employee | Same as above                                                                                              | Same as above                                                                                             |
| Da. M. Office work study employee | Same as above                                                                                              | Same as above                                                                                             |
| Al. P. Office work study employee | Same as above                                                                                              | Same as above                                                                                             |
| Ab. A. Sterilization w.s. employee | None, although they may see charts open or computer information when they work in and around the clinic. | HIPAA Training                                                                                           |
| K. D. Sterilization w.s. employee | None, although they may see charts open or computer information when they work in and around the clinic. | HIPAA Training                                                                                           |
| S. H. Sterilization w.s. employee | None, although they may see charts open or computer information                                           | HIPAA Training                                                                                           |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Access Details</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>G. M.</td>
<td>Sterilization w.s. employee</td>
<td>None, although they may see charts open or computer information when they work in and around the clinic</td>
<td>HIPAA Training</td>
</tr>
<tr>
<td>K. R.</td>
<td>Sterilization w.s. employee</td>
<td>None, although they may see charts open or computer information when they work in and around the clinic</td>
<td>HIPAA Training</td>
</tr>
<tr>
<td>Al. S.</td>
<td>Sterilization w.s. employee</td>
<td>None, although they may see charts open or computer information when they work in and around the clinic</td>
<td>HIPAA Training</td>
</tr>
<tr>
<td>Name of workforce member</td>
<td>Patient Information Needed to do the job</td>
<td>Any conditions that apply to this access</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| C.A., RDH \nDH Faculty \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| N.B., RDH \nDH Clinical Dental Hygienist \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| K.B., RDH \nDH Program Coordinator \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| D.B. \nDH Clinic Facilities Coordinator \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| S.B., RDH \nDH Faculty \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| D.B., RDH \nDH Clinical Dental Hygienist \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| K.H., RDH \nDH Faculty \nFull time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| A.J., RDH \nDH Clinic Operations Supervisor \nFull time | • Administrator and full access to electronic dental software  
• Full access to paper charts | • HIPAA training  
• EagleSoft training and customized access |
| C.M. | **Administrator** | • HIPAA training |
| **C.M.**  
Clinic Clerk, Full time  
Full time | • Administrator and full access to electronic dental software  
• Full access to paper charts | • EagleSoft training and customized access |
|---|---|---|
| **T.R., RDH**  
Department Head  
Does Not Work in Clinic | No access | No access |
| **L.S., RDH**  
DH Clinical Dental Hygienist  
Full time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
| **S.W., RDH**  
DH Faculty  
Full time | • Full access to paper charts  
• Customized access in dental software  
• No access to software financial component | • HIPAA training  
• EagleSoft training and customized access |
<table>
<thead>
<tr>
<th>Name of workforce member</th>
<th>Patient Information Needed to do the job</th>
<th>Any conditions that apply to this access</th>
</tr>
</thead>
<tbody>
<tr>
<td>J. C., RDH</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Clinic Instructor</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>V. F., RDH</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Clinic Instructor</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>S. F., RDH</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Clinic Instructor</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>Ar. G., RDH</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct DH Radiology Instructor</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>Au.G., DDS</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Dentist</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>M. G., RDH</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Clinic Instructor</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>T. H., DDS</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Dentist</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>R. N., RDH</td>
<td>• Full access to paper charts</td>
<td>• HIPAA training</td>
</tr>
<tr>
<td>Adjunct Clinic Instructor</td>
<td></td>
<td>• EagleSoft training and customized access</td>
</tr>
<tr>
<td>Part time</td>
<td>• Customized access in dental software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No access to software financial component</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Position</td>
<td>Full Access</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>J. K., RDH</td>
<td>Adjunct Clinic Instructor</td>
<td>Full access to paper charts</td>
</tr>
<tr>
<td>Ch. T., DDS</td>
<td>Adjunct Dentist</td>
<td>Full access to paper charts</td>
</tr>
<tr>
<td>Co. S., DDS</td>
<td>Adjunct Dentist</td>
<td>Full access to paper charts</td>
</tr>
<tr>
<td>Be. W., RDH</td>
<td>Clinic Clerk, Part-time</td>
<td>Full access to paper charts</td>
</tr>
<tr>
<td>S. H, DDS</td>
<td>Clinic Clerk, Part-time</td>
<td>Full access to paper charts</td>
</tr>
</tbody>
</table>
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

ROUTINE DISCLOSURES AND REQUESTS FORM

(This form is to be used to document minimum necessary levels for routine disclosure and requests of patient information)

For use when our dental practice makes a routine disclosure of patient information to a third party.

This list was created on _________________________________, 20 __________.
And was in effect until _________________________________, 20 __________.

<table>
<thead>
<tr>
<th>Type of routine disclosure</th>
<th>Patient information that may be disclosed without checking with the Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For use when our dental practice makes a routine request for patient information from a third party

This list was created on _________________________________, 20 __________.
And was in effect until _________________________________, 20 __________.

<table>
<thead>
<tr>
<th>Type of routine disclosure</th>
<th>Patient information that may be disclosed without checking with the Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Minimum necessary does not apply in the following situations:

- Disclosing patient information to a health care provider
- Requesting patient information from a health care provider for treatment
- Disclosing a patient’s information to the patient
- When a patient has signed an authorization form for the use or disclosure
- Disclosures to the U.S. Department of Health and Human Services
- Uses and disclosures required by law
- Uses and disclosures required in order to comply with the Privacy Rule

Unless one of the above exceptions applies, our dental practice will not access, use, disclose or request a patient’s entire dental record unless the entire dental record is needed to accomplish the purpose of the use, disclosure or request.
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

VERIFICATION OF IDENTITY FORM

(This form serves to document the verification of identity and authority of the person requesting patient information)

Please provide us with the following information.

Name of patient whose information you are requesting:

__________________________________________________________________________________________________________

__________________________________________________________________________________________________________

Patient’s Date of Birth: __________________________________________________________________

The specific patient information you are requesting:

__________________________________________________________________________________________________________

__________________________________________________________________________________________________________

Your Name: ___________________________________________________________________________

Address: _____________________________________________________________________________

City: _____________________________________ State: ______________ Zip: ____________________

Describe your authority to access this information:

_____________________________________________________________________________________

If you are a patient’s personal representative:

Relationship to Patient: ______________________________________________________________________________________

I certify that the above information is correct.

Signature: ___________________________ Date: __________________________

Dental Staff: Describe documentation presented by the requester:

____________________________________________________________________________________

EXPLANATION OF REQUIRED DISCLOSURE

Source: ADA Practical Guide to HIPAA Compliance, Chapter 2, pp 30

STEP 7: Required Disclosures
Understand which disclosures are required by HIPAA

Where to find the rules:

45 CFR 164.502(a)(2)

HIPAA requires that our dental practice disclose patient information in the following situations:

- When a patient (or a patient’s personal representative) asks to see or get copies of the patient’s information (Chapter 2, Step 14.1)
- When a patient (or a patient’s personal representative) asks for an accounting of disclosures (Chapter 2, Step 14.3)
- When the U.S. Department of Health and Human Services (HHS) requires patient information in order to investigate or determine the compliance with HIPAA.

In these situations, the dental practice does not need to have the patient sign an authorization form (Chapter 2, Step 9) before the dental practice makes the disclosure.

The minimum necessary requirement does not apply to these situations (Chapter 2, Step 5).
At A Glance – May I disclose protected health information for public health emergency preparedness purposes?

See flow chart:

S:\HIPAA Shared\Emergency PHI Disclosure Decision Tool
This form is for obtaining and documenting authorization for a use or disclosure of patient information that is not permitted or required by HIPAA.

Patient Name: _______________________________________________________________________

Patient’s Date of Birth: _____________________________ Patient’s Chart Number: ________

I hereby authorize the use and disclosure of the patient information as described below. I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

Specific description of the patient information to be used or disclosed:

_____________________________________________________________________________________

_____________________________________________________________________________________

_____________________________________________________________________________________

Purposes of this use or disclosure: _________________________________________________________

Is this authorization at the request of the individual or personal representative? YES NO (circle one)

I authorize the following person(s) to make this use or disclosure:

_____________________________________________________________________________________

_____________________________________________________________________________________

The following person(s) may receive this patient information:

_____________________________________________________________________________________

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice’s Privacy Officer at Ferris State University Dental Hygiene Clinic. I understand that my revocation must be in writing. If I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written revocation.

I understand that I may refuse to sign this authorization, and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits.
This authorization expires on the following date, or when the event occurs:

_____________________________________________________________________________________

Signature of Patient or Patient’s Personal Representative:

________________________________________ Date: ____________________________

If Personal Representative:

Print Name: _______________________________________________________________________

Signature: _______________________________________________________________________

Relationship to Patient: _____________________________________________________________

_________________________________________________________________________________

For Office Use Only

_________________________________________________________________________________

Copy of signed authorization provided to the individual:

Date: ______________

Initials: ____________

Core Elements Needed (Check as completed):

☐ Description of the information to be used or disclosed that ID’s the information in a specific
   and meaningful manner
☐ The name of the specific ID of the person(s) or class of persons authorized to make the
   requested use or disclosure.
☐ The name or other ID of the person(s) or class of persons to whom the dental practice may
   make the requested use or disclosure.
☐ A description of each purpose of the requested use or disclosure. The statement “At the
   request of the individual” is a sufficient description of the purpose when an individual initiates
   the authorization and does not provide a statement of purpose.
☐ An expiration date or an expiration event that relates to the individual or the purpose of the
   use or disclosure.
☐ Signature of the individual and date. If the authorization is signed by a personal
   representative of the individual, a description of such representative’s authority to act for the
   individual must be provided.
BUSINESS ASSOCIATE AGREEMENT
(for use when there is no written agreement with the business associate)

This HIPAA Business Associate Agreement (“Agreement”) is entered into this _______ day of ____________, 20__, by and between ______________________ (“Business Associate”) and ___________________________ (“Covered Entity”).

Business Associate provides __________________ services.

Covered Entity is a health care provider. Pursuant to federal laws and regulations, including the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Covered Entity has an obligation to protect certain health information of its customers (“Protected Health Information”). As part of this obligation, Covered Entity must receive assurances from any business associate who receives or has access to Covered Entity’s Protected Health Information that the business associate will protect the information in the same way as Covered Entity.

In performing services for Covered Entity, Business Associate may receive, access or create Protected Health Information on behalf of Covered Entity.

In consideration for Business Associate’s access to and/or use of Protected Health Information for those purposes allowed by HIPAA and consistent with the services that Business Associate performs for Covered Entity, and in consideration for the mutual promises and covenants set forth below, the parties agree as follows:

1. Definitions. As used in this Agreement:

   1.1. “Breach Notification Standards” shall mean the HIPAA regulations governing notification in the case of breach of unsecured Protected Health Information as set forth at 45 CFR § Part 164, Subpart D, as they exist now or as they may be amended.

   1.2. “Designated Record Set” shall mean a group of records maintained by or for Covered Entity that is (i) the medical records and billing records about individuals maintained by or for Covered Entity, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Covered Entity to make decisions about individuals. As used herein, the term “Record” means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for Covered Entity.

   1.3. “HIPAA” shall mean the Health Insurance Portability and Accountability Act, Public Law 104-91, and any amendments thereto.

   1.4. “HIPAA Transaction” shall mean Transactions as defined in 45 CFR § 160.103 of the Transaction Standards.
1.5. “HITECH Act” means the Health Information Technology for Economic and Clinical Health Act, found in the American Recovery and Reinvestment Act of 2009 at Division A, title XIII and Division B, Title IV.

1.6. “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.7. “Minimum Necessary” shall have the meaning set forth in the Health Information Technology for Economic and Clinical Health Act, § 13405(b).

1.8. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR § Part 160 and Part 164, as they exist now or as they may be amended.

1.9. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, limited to the information that Business Associate accesses, creates, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses on behalf of Covered Entity.

1.10. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.103.

1.11. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

1.12. “Security Standards” shall mean the Security Standards, 45 CFR § parts 160, 162 and 164, as they exist now or as they may be amended.

1.13. “Transaction Standards” shall mean the Standards for Electronic Transactions, 45 CFR § part 160 and part 162, as they exist now or as they may be amended.

1.14. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR §§160.103 and 164.501.

2. **Obligations and Activities of Business Associate.**

2.1. Business Associate agrees that it shall not, and that its directors, officers, employees, contractors and agents shall not, use or further disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.

2.2. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

2.3. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
2.4. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, or of any act or omission that violates the terms of this Agreement.

2.5. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees in writing to the terms of a business associate agreement containing the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.6. Business Associate agrees to provide access, within ten (10) days of receipt of such request to Protected Health Information in a Designated Record Set, to Covered Entity or, if requested by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

2.7. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, within ten (10) days of receipt of such request. If Business Associate provides Designated Record Sets to third parties, Business Associate shall ensure such records are also amended. [Not necessary if business associate does not have protected health information in a designated record set.]

2.8. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity, or at the request of Covered Entity to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity’s compliance with the Privacy Rule.

2.9. Business Associate agrees to document disclosures of Protected Health Information, and information related to such disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528 and any additional regulations promulgated by the Secretary pursuant to HITECH Act § 13405(c). Business Associate agrees to implement an appropriate record keeping process that will track, at a minimum, the following information: (i) the date of the disclosure; (ii) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person; (iii) a brief description of the Protected Health Information disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure.

2.10. Within twenty (20) days of receipt of such request Business Associate agrees to provide to Covered Entity or to an Individual, information collected in accordance with Section 2.9 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information during the six (6) years prior to the date on which the accounting was requested, in accordance with 45 CFR § 164.528.
2.11. In the event Business Associate receives a subpoena, court or administrative order or other discovery request or mandate for release of Protected Health Information, Business Associate will respond as permitted by 45 CFR § 164.512(e) and (f). Business Associate shall notify Covered Entity of the request as soon as reasonably practicable, but in any event within two (2) business days of receipt of such request.

2.12. Additionally, Business Associate will not make any communications in violation of the restrictions on marketing in 45 CFR § 164.508(a)(3).

2.13. If Business Associate will communicate with any individuals who are the subject of Protected Health Information originating from or prepared for Covered Entity, Business Associate agrees to implement procedures to give timely effect to an individual’s request to receive communications of Protected Health Information by alternative means or at alternative locations, pursuant to 45 CFR § 164.522(b), so as to ensure that Protected Health Information will only be communicated to those individuals designated in such a request as authorized to receive the Protected Health Information. If Business Associate provides records to agents, including subcontractors, who may also communicate with the individual, Business Associate shall ensure that the individual’s request for communications by alternative means is provided to and given timely effect by such agents.

2.14. Business Associate shall not directly or indirectly receive or provide remuneration in exchange for any Protected Health Information in violation of 45 CFR § 164.502(a)(5)(ii).

2.15. Upon request from Covered Entity, Business Associate shall permit Covered Entity to review and audit Business Associate’s policies, procedures and practices relating to the use and protection of Protected Health Information, including the right to audit contracts and relationships with agents and subcontractors who have access to Protected Health Information and upon request shall provide Covered Entity with copies of relevant documents.

2.16. **Electronic Transactions.** Business Associate hereby represents and warrants that, to the extent that it is electronically transmitting any of the HIPAA Transactions for Health Plan Sponsor, the format and structure of such transmissions shall be in compliance with the Transaction Standards.

2.17. **Electronic Data Security.** To the extent that Business Associate creates, receives, maintains or transmits electronic Protected Health Information, Business Associate hereby represents and warrants that it:

2.17.1. Has implemented and documented administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity consistent with the requirements at 45 CFR Part 164, Subpart C;

2.17.2. Will ensure that any agent, including a subcontractor, to whom Business Associate provides electronic Protected Health Information agrees to sign a business associate agreement and implements reasonable and appropriate safeguards to protect the Protected Health Information; and
2.17.3. Will keep records of all security incidents involving Protected Health Information of which Business Associate becomes aware, and will report to Covered Entity all significant security incidents of which Business Associate becomes aware.

2.18. Breach Notification. Business Associate warrants that it has in place policies and procedures that are designed to detect inappropriate acquisition, access, use or disclosure of Protected Health Information and that it adequately trains its work force and agents on these procedures. Business Associate will notify Covered Entity within three (3) business days of discovering an acquisition, access, use or disclosure of Protected Health Information in a manner or for a purpose not permitted by the HIPAA Privacy Rule and within 30 calendar days of discovery will provide Covered Entity with the identification of each individual whose Protected Health Information has been or is reasonably believed by Business Associate to have been acquired, accessed, used or disclosed during such incident. Business Associate will assist Covered Entity in assessing whether the impermissible acquisition, access, use or disclosure of Protected Health Information compromises the security or privacy of such Protected Health Information. If Covered Entity determines that individuals whose data is affected by the impermissible acquisition, access, use or disclosure must be notified pursuant to the HIPAA Breach Notification Standards or other applicable law, Business Associate will reimburse Covered Entity’s reasonable notification costs, including legal fees and other costs associate with determining its notification duty, drafting its notification letter, mailing the notification letter and staffing its call center.

3. Permitted Uses and Disclosures by Business Associate

3.1. General Use. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of or to provide services to Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: [List permitted purposes] In performing such services, Business Associate will comply with all Privacy Rule requirements that would apply to Covered Entity if Covered Entity were performing such services.

3.2. Specific Use and Disclosure Provisions

3.2.1. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

3.2.2. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
3.2.3. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

4. **Obligations of Covered Entity.**

4.1. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of Protected Health Information. Business Associate will give timely effect to such limitations.

4.2. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate’s use or disclosure of Protected Health Information. Business Associate will give timely effect to such changes or revocations.

4.3. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of Protected Health Information. Business Associate will give timely effect to such restrictions.

4.4. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except as specifically allowed by section 3.2 of this Agreement.

5. **Term and Termination.**

5.1. **Term.** The Term of this Agreement shall be effective as of the date it is executed, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

5.2. **Termination for Breach by Business Associate.** Upon Covered Entity’s knowledge of a material breach of the terms of this Agreement by Business Associate, Covered Entity shall either:

5.2.1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate their relationship and this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

5.2.2. Immediately terminate its relationship with Business Associate and this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.
5.3. **Other Conditions Allowing for Immediate Termination.** Notwithstanding anything to the contrary in this Agreement, Covered Entity may terminate its relationship with Business Associate and this Agreement immediately upon written notice to Business Associate, without any notice period and/or judicial intervention being required, and without liability for such termination, in the event that:

5.3.1. Business Associate (i) receives a Criminal Conviction, (ii) is excluded, barred or otherwise ineligible to participate in any government health care program, including but not limited to Medicare, Medicaid or Tricare; (iii) is named as a defendant in a criminal proceeding for a violation of any information privacy and protection law; or (iv) is found to have or stipulates that it has violated any privacy, security or confidentiality protection requirements under any applicable information privacy and protection law in any administrative or civil proceeding in which Business Associate has been joined.;

5.3.2. A trustee or receiver is appointed for any or all property of Business Associate;

5.3.3. Business Associate becomes insolvent or unable to pay debts as they mature, or ceases to so pay, or makes an assignment for benefit of creditors;

5.3.4. Bankruptcy or insolvency proceedings under bankruptcy or insolvency code or similar law, whether voluntary or involuntary, are properly commenced by or against Business Associate;

5.3.5. Business Associate is dissolved or liquidated.

5.4. **Effect of Termination.**

5.4.1. Except as provided in paragraph 5.4.2 of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

5.4.2. In the event that return or destruction of the Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. **Miscellaneous.**

6.1. **Amendment.** No provision of this Agreement may be modified except by a written document signed by a duly authorized representative of the parties. The parties agree to amend this Agreement, as appropriate, to conform with any new or revised legislation, rules and regulations to which Covered Entity is subject now or in the future including, without limitation, the Privacy Rule, Security Standards or Transactions Standards (collectively "Laws"). If within
ninety (90) days of either party first providing written notice to the other of the need to amend this Agreement to comply with Laws, the parties, acting in good faith, are i) unable to mutually agree upon and make amendments or alterations to this Agreement to meet the requirements in question, or ii) alternatively, the parties determine in good faith that amendments or alterations to the requirements are not feasible, then either party may terminate this Agreement upon thirty (30) days written notice.

6.2. **Assignment.** No party may assign or transfer any or all of its rights and/or obligations under this Agreement or any part of it, nor any benefit or interest in or under it, to any third party without the prior written consent of the other party, which shall not be reasonably withheld.

6.3. **Survival.** The respective rights and obligations of Business Associate under Section 5.4 of this Agreement shall survive the termination of this Agreement.

6.4. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Breach Notification Standards, Privacy Rule, Security Standards, and Transaction Standards. If there is any inconsistency between this Agreement and any other agreement between the parties, the language in this Agreement shall control.

6.5. **Right to Cure.** In addition to any other rights Covered Entity may have in this Agreement, or by operation of law or in equity, if Covered Entity determines that Business Associate has violated a material term of this Agreement, Covered Entity may, at its option, cure or end any such violation. Covered Entity's cure of a breach of this Agreement shall not be construed as a waiver of any other rights Covered Entity has in this Agreement or by operation of law or in equity.

6.6. **Indemnification.** Business Associate shall indemnify and hold harmless Covered Entity for any and all claims, inquiries, costs or damages, including but not limited to any monetary penalties, that Covered Entity incurs arising from a violation by Business Associate of its obligations hereunder.

6.7. **Exclusion from Limitation of Liability.** To the extent that Business Associate has entered into other agreements with Covered Entity in which Business Associate has limited its liability, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect or punitive damages, or other such limitations, such limitations shall exclude all damages to Covered Entity arising from Business Associate's breach of its obligations relating to the use and disclosure of Protected Health Information under this Agreement.

6.8. **Third Party Rights.** The terms of this Agreement are not intended, nor should they be construed, to grant any rights to any parties other than Business Associate and Covered Entity.

6.9. **Minimum Necessary.** Business Associate hereby represents and warrants that, for all Protected Health Information that Business Associate accesses or requests from Covered Entity for the purposes of providing services, it shall access or request only that amount of information that is minimally necessary to perform such services. In addition, for all uses and disclosures of Protected Health Information by Business Associate, Business Associate represents and warrants that it shall institute and implement policies and practices to limit such uses and disclosures to that
which is minimally necessary to perform its services. Business Associate shall determine the amount minimally necessary consistent with the requirements in 45 CFR § 164.502(b).

6.10. **Compliance.** Business Associate may use and disclose Protected Health Information only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 CFR 164 Subpart E, as required under 45 CFR 164.500(c) and 45 CFR § 164.504(e)(2)(ii)(H) and this Agreement.

6.11. **Injunctive Relief.** Business Associate acknowledges and stipulates that its unauthorized use or disclosure of Protected Health Information while performing services would cause irreparable harm to Covered Entity, and in such event, Covered Entity shall be entitled, if it so elects, to institute and prosecute proceedings in any court of competent jurisdiction, either in law or in equity, to obtain damages and injunctive relief, together with the right to recover from Business Associate costs, including reasonable attorneys' fees, for any such breach of the terms and conditions of this Agreement.

6.12. **Notice.** All notices required under this Agreement shall be in writing and shall be deemed to have been given on the next day by fax or other electronic means or upon personal delivery, or in ten (10) days upon delivery in the mail, first class, with postage prepaid. Notices shall be sent to the addressees indicated below unless written notification of change of address shall have been given.

If to Covered Entity

_________________________________

_________________________________

_________________________________

Tel: _____________________________

Fax:___________________________

If to Business Associate:

_________________________________

_________________________________

_________________________________

Tel: ________________________________

Fax: _______________________________

6.13. **Owner of Protected Health Information.** Under no circumstances shall Business Associate be deemed in any respect to be the owner of any Protected Health Information used or disclosed by or to Business Associate.
IN WITNESS WHEREOF, the parties have executed this Agreement the day and year first written above.

BUSINESS ASSOCIATE:

Signed

Printed

Date

COVERED ENTITY:

Signed

Printed

Date
BUSINESS ASSOCIATE ADDENDUM

[To be used whenever Covered Entity already has a written contract with a business associate; this addendum incorporates HIPAA’s Privacy Rule and Security Rule requirements into the existing agreement]

This HIPAA Addendum (“Addendum”) is entered into this ______ day of ____________, 20__, by and between ______________________ (“Business Associate”) and ____________________ (“Covered Entity”) and amends the __________________ Agreement (“Agreement”) previously entered into between Business Associate and Covered Entity.

Covered Entity is a health care provider. Pursuant to federal laws and regulations, including the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Covered Entity has an obligation to protect certain health information of its customers (“Protected Health Information”). As part of this obligation, Covered Entity must receive assurances from any business associate who receives or has access to Covered Entity’s Protected Health Information that the business associate will protect the information in the same way as Covered Entity.

In performing services for Covered Entity, Business Associate may receive, access or create Protected Health Information on behalf of Covered Entity.

In consideration for Business Associate’s access to and/or use of Protected Health Information for those purposes allowed by HIPAA and consistent with the terms of the Agreement, Business Associate and Covered Entity agree as follows:

1. **Definitions.** As used in this Addendum:

   1.1. “Breach Notification Standards” shall mean the HIPAA regulations governing notification in the case of breach of unsecured Protected Health Information as set forth at 45 CFR § Part 164, Subpart D, as they exist now or as they may be amended.

   1.2. “Designated Record Set” shall mean a group of records maintained by or for Covered Entity that is (i) the medical records and billing records about individuals maintained by or for Covered Entity, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Covered Entity to make decisions about individuals. As used herein, the term “Record” means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for Covered Entity.

   1.3. “HIPAA” shall mean the Health Insurance Portability and Accountability Act, Public Law 104-91, and any amendments thereto.
1.4. “HIPAA Transaction” shall mean Transactions as defined in 45 CFR § 160.103 of the Transaction Standards.

1.5. “HITECH Act” means the Health Information Technology for Economic and Clinical Health Act, found in the American Recovery and Reinvestment Act of 2009 at Division A, title XIII and Division B, Title IV.

1.6. “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.7. “Minimum Necessary” shall have the meaning set forth in the Health Information Technology for Economic and Clinical Health Act, § 13405(b).

1.8. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR § Part 160 and Part 164, as they exist now or as they may be amended.

1.9. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, limited to the information that Business Associate accesses, creates, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses on behalf of Covered Entity.

1.10. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.103.

1.11. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

1.12. “Security Standards” shall mean the Security Standards, 45 CFR § parts 160, 162 and 164, as they exist now or as they may be amended.

1.13. “Transaction Standards” shall mean the Standards for Electronic Transactions, 45 CFR § part 160 and part 162, as they exist now or as they may be amended.

1.14. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in 45 CFR §§ 160.103 and 164.501.

2. **Obligations and Activities of Business Associate.**

2.1. Business Associate agrees that it shall not, and that its directors, officers, employees, contractors and agents shall not, use or further disclose Protected Health Information other than as permitted or required by this Addendum or as Required By Law.

2.2. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Addendum.
2.3. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Addendum.

2.4. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Addendum of which it becomes aware, or of any act or omission that violates the terms of this Addendum.

2.5. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees in writing to the terms of a business associate agreement containing the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

2.6. Business Associate agrees to provide access, within ten (10) days of receipt of such request to Protected Health Information in a Designated Record Set, to Covered Entity or, if requested by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

2.7. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual within ten (10) days of receipt of such request. If Business Associate provides Designated Record Sets to third parties, Business Associate shall ensure such records are also amended. [Not necessary if business associate does not have protected health information in a designated record set.]

2.8. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity, or at the request of Covered Entity to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity’s compliance with the Privacy Rule.

2.9. Business Associate agrees to document disclosures of Protected Health Information, and information related to such disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528 and any additional regulations promulgated by the Secretary pursuant to HITECH Act § 13405(c). Business Associate agrees to implement an appropriate record keeping process that will track, at a minimum, the following information: (i) the date of the disclosure; (ii) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person; (iii) a brief description of the Protected Health Information disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure.

2.10. Within twenty (20) days of receipt of such request Business Associate agrees to provide to Covered Entity or to an Individual, information collected in accordance with Section
2.9 of this Addendum, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information during the six (6) years prior to the date on which the accounting was requested, in accordance with 45 CFR § 164.528.

2.11. In the event Business Associate receives a subpoena, court or administrative order or other discovery request or mandate for release of Protected Health Information, Business Associate will respond as permitted by 45 CFR § 164.512(e) and (f). Business Associate shall notify Covered Entity of the request as soon as reasonably practicable, but in any event within two (2) business days of receipt of such request.

2.12. Business Associate will not make any communications in violation of the restrictions on marketing in 45 CFR § 164.508(a)(3).

2.13. If Business Associate will communicate with any individuals who are the subject of Protected Health Information originating from or prepared for Covered Entity, Business Associate agrees to implement procedures to give timely effect to an individual’s request to receive communications of Protected Health Information by alternative means or at alternative locations, pursuant to 45 CFR § 164.522(b), so as to ensure that Protected Health Information will only be communicated to those individuals designated in such a request as authorized to receive the Protected Health Information. If Business Associate provides records to agents, including subcontractors, who may also communicate with the individual, Business Associate shall ensure that the individual’s request for communications by alternative means is provided to and given timely effect by such agents.

2.14. Business Associate shall not directly or indirectly receive or provide remuneration in exchange for any Protected Health Information in violation of 45 CFR § 164.502(a)(5)(ii).

2.15. Upon request from Health Plan Sponsor, Business Associate shall permit Health Plan Sponsor to review and audit Business Associate’s policies, procedures and practices relating to the use and protection of Protected Health Information, including the right to audit contracts and relationships with agents and subcontractors who have access to Protected Health Information, and upon request shall provide Covered Entity with copies of relevant documents.

2.16. **Electronic Transactions.** Business Associate hereby represents and warrants that, to the extent that it is electronically transmitting any of the HIPAA Transactions for Covered Entity, the format and structure of such transmissions shall be in compliance with the Transaction Standards.

2.17. **Electronic Data Security.** To the extent that Business Associate creates, receives, maintains or transmits electronic Protected Health Information, Business Associate hereby represents and warrants that it:

2.17.1. Has implemented and documented administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity consistent with the requirements at 45 CFR §§ 164.306, 164.308, 164.310, 164.312 and 164.316;
2.17.2. Will ensure that any agent, including a subcontractor, to whom Business Associate provides electronic Protected Health Information agrees to sign a business associate agreement and implements reasonable and appropriate safeguards to protect the Protected Health Information; and

2.17.3. Will keep records of all security incidents involving Protected Health Information of which Business Associate becomes aware, and will report to Covered Entity all significant security incidents of which Business Associate becomes aware.

2.18. **Breach Notification**. Business Associate warrants that it has in place policies and procedures that are designed to detect inappropriate acquisition, access, use or disclosure of Protected Health Information and that it adequately trains its work force and agents on these procedures. Business Associate will notify Covered Entity within three (3) business days of discovering an acquisition, access, use or disclosure of Protected Health Information in a manner or for a purpose not permitted by the HIPAA Privacy Rule and within 30 calendar days of discovery will provide Covered Entity with the identification of each individual whose Protected Health Information has been or is reasonably believed by Business Associate to have been acquired, accessed, used or disclosed during such incident. Business Associate will assist Covered Entity in assessing whether the impermissible acquisition, access, use or disclosure of Protected Health Information compromises the security or privacy of such Protected Health Information. If Covered Entity determines that individuals whose data is affected by the impermissible acquisition, access, use or disclosure must be notified pursuant to the HIPAA Breach Notification Standards or other applicable law, Business Associate will reimburse Covered Entity’s reasonable notification costs, including legal fees and other costs associate with determining its notification duty, drafting its notification letter, mailing the notification letter and staffing its call center.

3. **Permitted Uses and Disclosures by Business Associate**

3.1. **General Use.** Except as otherwise limited in this Addendum, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity. In performing such services, Business Associate will comply with all Privacy Rule requirements that would apply to Covered Entity if Covered Entity were performing such services.

3.2. **Specific Use and Disclosure Provisions**

3.2.1. Except as otherwise limited in this Addendum, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

3.2.2. Except as otherwise limited in this Addendum, Business Associate may disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the
purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.2.3. Except as otherwise limited in this Addendum, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

4. **Obligations of Covered Entity.**

4.1. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitations may affect Business Associate’s use or disclosure of Protected Health Information. Business Associate will give timely effect to such limitations.

4.2. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate’s use or disclosure of Protected Health Information. Business Associate will give timely effect to such changes or revocations.

4.3. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of Protected Health Information. Business Associate will give timely effect to such restrictions.

4.4. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except as specifically allowed by section 3.2 of this Addendum.

5. **Term and Termination.**

5.1. **Term.** This Addendum shall be effective as of the date it is executed, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

5.2. **Termination for Breach by Business Associate.** Upon Covered Entity’s knowledge of a material breach of the terms of this Addendum by Business Associate, Covered Entity shall either:

5.2.1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement and this Addendum if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
5.2.2. Immediately terminate the Agreement and this Addendum if Business Associate has breached a material term of this Addendum and cure is not possible.

5.3. Other Conditions Allowing for Immediate Termination. Notwithstanding anything to the contrary in the Agreement or this Addendum, Covered Entity may terminate the Agreement and this Addendum immediately upon written notice to Business Associate, without any term of notice and/or judicial intervention being required, and without liability for such termination, in the event that:

5.3.1. Business Associate (i) receives a Criminal Conviction, (ii) is excluded, barred or otherwise ineligible to participate in any government health care program, including but not limited to Medicare, Medicaid or Tricare; (iii) is named as a defendant in a criminal proceeding for a violation of any information privacy and protection law; or (iv) is found to have or stipulates that it has violated any privacy, security or confidentiality protection requirements under any applicable information privacy and protection law in any administrative or civil proceeding in which Business Associate has been joined.;

5.3.2. A trustee or receiver is appointed for any or all property of Business Associate;

5.3.3. Business Associate becomes insolvent or unable to pay debts as they mature, or ceases to so pay, or makes an assignment for benefit of creditors;

5.3.4. Bankruptcy or insolvency proceedings under bankruptcy or insolvency code or similar law, whether voluntary or involuntary, are properly commenced by or against Business Associate;

5.3.5. Business Associate is dissolved or liquidated.

5.4. Effect of Termination.

5.4.1. Except as provided in paragraph 5.4.2 of this section, upon termination of the Agreement or this Addendum, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

5.4.2. In the event that return or destruction of the Protected Health Information is infeasible, Business Associate shall extend the protections of this Addendum to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. Miscellaneous.
6.1. **Amendment.** No provision of this Addendum may be modified except by a written document signed by a duly authorized representative of the parties. The parties agree to amend either the Agreement or this Addendum, as appropriate, to conform with any new or revised legislation, rules and regulations to which Covered Entity is subject now or in the future including, without limitation, the Privacy Rule, Security Standards or Transactions Standards (collectively "Laws"). If within ninety (90) days of either party first providing written notice to the other of the need to amend the Agreement or Addendum to comply with Laws, the parties, acting in good faith, are i) unable to mutually agree upon and make amendments or alterations to the Agreement or Addendum to meet the requirements in question, or ii) alternatively, the parties determine in good faith that amendments or alterations to the requirements are not feasible, then either party may terminate the Agreement upon thirty (30) days written notice.

6.2. **Assignment.** No party may assign or transfer any or all of its rights and/or obligations under this Addendum or any part of it, nor any benefit or interest in or under it, to any third party without the prior written consent of the other party, which shall not be reasonably withheld.

6.3. **Survival.** The respective rights and obligations of Business Associate under section 5.4 of this Addendum shall survive the termination of this Addendum.

6.4. **Interpretation.** Any ambiguity in this Addendum shall be resolved to permit Covered Entity to comply with the Breach Notification Standards, Privacy Rule, Security Standards, and Transaction Standards. If there is an inconsistency between the language in the Agreement and this Addendum, the language in this Addendum shall control.

6.5. **Right to Cure.** In addition to any other rights Covered Entity may have in the Agreement, this Addendum, or by operation of law or in equity, if Covered Entity determines that Business Associate has violated a material term of this Addendum, Covered Entity may, at its option, cure or end any such violation. Covered Entity’s cure of a breach of this Addendum shall not be construed as a waiver of any other rights Covered Entity has in the Agreement, this Addendum or by operation of law or in equity.

6.6. **Indemnification.** Business Associate shall indemnify and hold harmless Covered Entity for any and all claims, inquiries, costs or damages, including but not limited to any monetary penalties, that Covered Entity incurs arising from a violation by Business Associate of its obligations hereunder.

6.7. **Exclusion from Limitation of Liability.** To the extent that Business Associate has limited its liability under the terms of the Agreement, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect or punitive damages, or other such limitations, all limitations shall exclude all damages to Covered Entity arising from Business Associate’s breach of its obligations relating to the use and disclosure of Protected Health Information.

6.8. **Third Party Rights.** The terms of this Addendum are not intended, nor should they be construed, to grant any rights to any parties other than Business Associate and Covered Entity.
6.9. **Minimum Necessary.** Business Associate hereby represents and warrants that, for all Protected Health Information that Business Associate accesses or requests from Covered Entity for the purposes of providing services under the Agreement, it shall access or request only that amount of information that is minimally necessary to perform such services. In addition, for all uses and disclosures of Protected Health Information by Business Associate, Business Associate represents and warrants that it shall institute and implement policies and practices to limit such uses and disclosures to that which is minimally necessary to perform its services under the Agreement. Business Associate shall determine the amount minimally necessary consistent with the requirements in 45 CFR § 164.502(b).

6.10. **Compliance.** Business Associate may use and disclose Protected Health Information only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 CFR 164 Subpart E, as required under 45 CFR § 164.500(c) and 45 CFR § 164.504(e)(2)(ii)(H) and this Addendum.

6.11. **Injunctive Relief.** Business Associate acknowledges and stipulates that its unauthorized use or disclosure of Protected Health Information while performing services pursuant to the Agreement or this Addendum would cause irreparable harm to Covered Entity, and in such event, Covered Entity shall be entitled, if it so elects, to institute and prosecute proceedings in any court of competent jurisdiction, either in law or in equity, to obtain damages and injunctive relief, together with the right to recover from Business Associate costs, including reasonable attorneys' fees, for any such breach of the terms and conditions of the Agreement or this Addendum.

6.12. **Notice.** All notices required under this Addendum shall be in writing and shall be deemed to have been given on the next day by fax or other electronic means or upon personal delivery, or in ten (10) days upon delivery in the mail, first class, with postage prepaid. Notices shall be sent to the addressees indicated below unless written notification of change of address shall have been given.

If to Covered Entity: If to Business Associate:

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

Tel: ___________________________ Tel: ___________________________

Fax: ___________________________ Fax: ___________________________

6.13. **Owner of Protected Health Information.** Under no circumstances shall Business Associate be deemed in any respect to be the owner of any Protected Health Information used or disclosed by or to Business Associate pursuant to the terms of the Agreement or this Addendum.
IN WITNESS WHEREOF, the parties have executed this Addendum the day and year first written above.

BUSINESS ASSOCIATE:

Signed

Printed

Date

COVERED ENTITY:

Signed

Printed

Date

9092431
REQUEST FOR ACCESS FORM

The purpose of this form is to document a request for access to patient information.

Privacy Officer Name: DH Clinic Operations Supervisor Telephone: 231-591-2260

Patient’s Name: (print)______________________________________________________________

Date of Birth: ___________________________________________________(for identification purposes)

Describe the records you wish to access and the approximate dates of the records:
_____________________________________________________________________________________
_____________________________________________________________________________________  
_____________________________________________________________________________________
_____________________________________________________________________________________

What would you like for us to do for you?

☐ I wish to see the requested records
☐ I wish to get a copy of the requested records
☐ I wish to see and get a copy of the requested records
☐ If the requested records are in an electronic designated record set, I wish an electronic copy of
  the requested records in the following format, if readily producible:
  _______________________________________________________________________________________
  _______________________________________________________________________________________
  _______________________________________________________________________________________
  _______________________________________________________________________________________
  If you would like the information emailed, enter the email address here (PLEASE PRINT VERY
  CLEARLY!) __________________________________________________________________________

  We do not recommend sending patient information in an unencrypted email because third
  parties may be able to access the email.

☐ I want you to prepare a summary of the requested records and I agree in advance to pay a fee in
  the amount of $__________.
☐ I want you to prepare an explanation of the records that I saw or got a copy of, and I agree in
  advance to pay a fee in the amount of $__________.

(See back of form for more information)
☐ I want you to send the copy of the requested records to:

Name:
________________________________________________________________________

Address:
________________________________________________________________________

Fees

Our practice charges a reasonable, cost-based fee for the copies of patient information, and for postage to mail records if requested.

Questions?

Please contact our Privacy Officer listed at the top of this page if you have any questions about your privacy to inspect or copy records.

If the request is by a patient:

Patient Signature: ________________________________ Date: _______________________

If the request is by a patient’s personal representative:

Name of the Personal Representative: ________________________________

Relationship to Patient: ________________________________

I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above.

Signature of Personal Representative:
________________________________________________________________________ Date: _______________________

For Dental Office Use Only

May need to consult with FSU General Counsel prior to making a decision.

☐ Request for access denied (attach written denial)
☐ Request for access approved
REQUEST FOR AMENDMENT FORM

This form documents how the dental practice acquires a patient’s request to amend the patient’s protected health information in the patient’s designated record set.

To the Patient: Please use this form to ask our dental practice to change any information about you in our records. All requests for change to our records must be in writing and must state the reason for the change. You must return this form to the Privacy Officer listed on the bottom of this form.

Patient Information

Name of Patient (print name): ____________________________________________

Patient’s Date of Birth: _______________________ Today’s Date: ______________________________

Patient Signature: _________________________________ Date: ________________________________

For Personal Representative of the Patient:

Your Name: ___________________________________________________________________________

Your Relationship to Patient: _____________________________________________________________

Personal Representative Signature: _________________________________ Date: ________________

I hereby certify that I have legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: ______________________________ Date: ________________

Requested Amendment

Please describe in detail how you want your records changed:
_______________________________________________________________________________________

Reason for requested change:
_______________________________________________________________________________________

Contact Person

Please contact the dental practice’s Privacy Officer if you have any questions relating to your request to amend records.
Privacy Officer: Dental Hygiene Clinic Operations Supervisor

Address: Ferris State University, College of Health Professions, 200 Ferris Drive, Big Rapids, MI 49307

Telephone: 231-591-2260
DENIAL OF REQUEST TO AMEND FORM

This form documents how to notify a patient that the dental clinic has denied the patient’s request to amend information in a designated record set.

Patient’s Name: _______________________________________________________________________

Patient’s Address: ______________________________________________________________________

Dear _____________________________________ ,

We are responding to your request to amend patient information. We have reviewed the request carefully and we have determined that we cannot approve the amendment that you asked for.

The reason for the denial is as follows:

☐ The information or record is not in a designated record set
☐ The information or record is accurate and complete
☐ The patient does not have a right to access the information or record
☐ The dental practice did not create the information or record.

You have the right to give us a written statement disagreeing with this denial. The statement may not be longer than one page. If you would like to give us a statement, please mail it to our Privacy Officer at the address below. If you do not give us a statement of disagreement, you may ask us to give your request for amendment and our denial every time we disclose the information that you wanted us to amend.

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about your health information or in response to a request you made, you may file a complaint with our dental practice by contacting our Privacy Officer at the address below, or calling our Privacy Officer at 231-591-2260. You also may submit a written complaint to the U.S. Department of Health and Human Services. You can file your complaint with the U.S. Department of Health and Human Services by following the instructions on this web page:

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

If you have any questions about this notice, please contact:

Privacy Officer: Dental Hygiene Clinic Operations Supervisor

Address: Ferris State University, 200 Ferris Drive, Big Rapids, MI 49307

Telephone Number: 231-591-2260
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

AMENDMENT REQUEST LOG

This form documents the dental practice’s responses to patient requests to amend information in a designated record set.

<table>
<thead>
<tr>
<th>PATIENT NAME</th>
<th>AMENDMENT REQUESTED</th>
<th>APPROVED OR DENIED?</th>
<th>DATE AMENDMENT COMPLETED</th>
<th>LIST 3(^{RD}) PARTIES WHO MUST BE NOTIFIED OF THE AMENDMENT</th>
<th>DATE AMENDMENTS SENT TO 3(^{RD}) PARTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This form documents disclosures of patient information so that the dental practice is prepared in the event a patient asks for an accounting of patient disclosures.

<table>
<thead>
<tr>
<th>Patient Name</th>
<th>Date of Disclosure</th>
<th>Who received the information?</th>
<th>Description of PHI disclosed</th>
<th>Purpose of disclosure</th>
<th>Was the disclosure for research?</th>
<th>Is this one of multiple disclosures that can be grouped?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REQUEST FOR ACCOUNTING OF DISCLOSURE

This form documents a patient’s request for an accounting of disclosures of the patient’s protected health information.

**Notice to Patients:** Please use this form to make a request that our practice provide you with an accounting of disclosures of your protected health information.

**Patient Name:** ____________________________________________________________

**Patient DOB:** ________________________________ (For identification purposes)

**Disclosure Accounting Request**

**Time Frame**

Please specify the dates between which you would like for our practice to account for disclosures of your protected health information. Under HIPAA, we are not required to include certain disclosures, including disclosures for treatment, payment or healthcare operations.

**Starting Date for Disclosure:** ________________________________

**Ending Date for Disclosure:** ______________________________________________________

**Our Practice’s Contact Person**

Please contact the DH Clinic Operations Supervisor, our Practice’s Privacy Officer if you have any questions relating to your Accounting of Disclosure request.

**Patient Information**

**Print Name:** ________________________________________________________________

**Signature:** __________________________________________________________________

**Date:** ________________________________
REQUEST FOR CONFIDENTIAL COMMUNICATIONS

This form documents a patient’s request that the dental practice communicate with the patient in a different way or at a different place.

To the Patient: Use this form if you would like our dental practice to communicate with you other than at your primary phone number and/or address. Fill out this request in its entirety.

Patient Name (print): ___________________________________________________________________

Alternative Communication Request (Please tell us the way you would like us to communicate with you, and/or the address you would like us to use: __________________________
______________________________
______________________________

Payment Information
Your request may affect your normal billing and payment procedure. Please specify any alternative method for handling payment.

____________________________________________________________________________________
____________________________________________________________________________________

Caution: there is some level of risk that third parties might be able read unencrypted emails.

Patient Signature: __________________________________ Date: _______________________

For Personal Representatives of the Patient

Print Name of the Personal Representative: __________________________________________

Relationship to the Patient: ________________________________________________________
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

RESTRICTED USE OR DISCLOSURE FORM

Please check and complete either A or B, as applicable.

☐ A. Health Plan Restriction for items/services paid for in full.

Patient Name (please print): _____________________________________________

asks the dental practice not to give information about the following item(s) and/or service(s), for
which the dental practice has been paid in full, to the health plan indicated below, for purposes of
payment or health care operations, unless required by law:

Items(s) or service(s): ___________________________________________________________________

Health Plan: ___________________________________________________________________________

I understand that the dental practice must agree to this requested restriction if the practice has received
payment in full for these item(s) or service(s).

Patient Signature: ________________________________ Date: __________________________

Dental Practice: has payment in full been received?  Yes/No  (circle one)

Administrator’s Signature: ________________________________ Date: __________________________

☐ B. Other Restriction

Patient Name: _____________________________________________ (please print) asks the dental practice not
to use or disclose the information indicated below in the manner indicated below:

Description of information:
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

Requested restricted use and/or disclosure:
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

I understand that the FSU Dental Hygiene Clinic (FSU dental practice) is not required to agree to this
requested restriction, but that if the dental practice does agree it can end the restriction by telling me.  I
understand that if the dental practice agrees to the restriction, the dental practice may use and disclose the restricted information in certain circumstances, such as for public health disclosures.

Patient Signature: __________________________________________ Date: ______________________

Administrator’s Signature: ___________________________ Date: ______________________

For Dental Office Use Only

☐ Agree to

☐ Not Agree to

Note: The dental practice must agree to a request for disclosure to a health plan of information about a health care item or service for which the dental practice has been paid in full (see Section A of this form).

Signature: __________________________________________ Date: ______________________
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

HIPAA TRAINING SIGN IN SHEET

This form documents the dental practice’s workforce members receiving training.

Name of Trainer: _______________________________________________________________________

Trainer’s Company Affiliation: _______________________________________________________________________

Length of Training: ________________________________ Date of Training: ___________________

Topics included in Training:
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
(Attach outline)

ATTENDEE LIST

<table>
<thead>
<tr>
<th>PRINT NAME</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PATIENT BILL OF RIGHTS

Welcome to the Ferris Dental Hygiene Clinic. This facility provides the opportunity for our dental hygiene students to receive their clinical experience in preparation to become licensed professional dental hygienists. The services provided by the student dental hygienists are under the supervision of licensed dental hygienists and dentists.

These services include: extra and intraoral examination, blood pressure screening, oral hygiene evaluation and instruction, x-rays for diagnosis by a dentist, oral data gathering (periodontal probing, hard tissue charting), oral prophylaxis, topical fluoride applications, and pit and fissure sealants.

As a patient in the clinic, you are entitled to considerate, respectful and confidential treatment which meets the dental hygiene profession's standard of care. You should expect to be informed of the treatment recommended and alternatives, the option to refuse treatment, the risk of no treatment, and the expected outcomes of various treatments. You should expect to know the cost of the treatment in advance. You should expect to be kept informed on the status of your condition and the anticipated length of time for treatment to be completed.

The dental hygiene care that you receive is NOT a substitute for your regular, periodic examination at your own dentists. We encourage you to contact your dentist for a dental examination so that he/she can determine your additional dental needs.

_____________________________________________________________________________________

INFORMED CONSENT FOR DENTAL TREATMENT

I authorize the performance of dental services on____________________________________________

(myself or name of patient)

I have read the Clinic Information listed above. I understand that the services received here are not intended to replace a regular, periodic examination by my private dentist.

I understand that the dental procedures, the medical services rendered in conjunction therewith, and the post-operative care are to be performed and rendered by those individuals, including students, selected and deemed qualified by the dental teaching staff of Ferris State University.

I also authorize Ferris State University's medical and dental staff to administer anesthesia or medication as deemed necessary for my treatment.

I authorize Ferris State University to use my pictures, radiographs, records, models, or any reproductions of the same for the purpose of classroom illustration, publicity, or dental publication. I will hold Ferris State University free from any encumbrance or liability with respect to the above mentioned photographs, radiographs, records, models, or any reproduction of the same.

I authorize Ferris State University to release my x-rays or dental records to my private dentist as requested. I agree that Ferris State University Dental Hygiene Clinic may send my radiographs in an electronic format and, at my request, will send them to the email address provided by the dentist of my choice. I am aware that there is some level of risk that third parties might be able to read unencrypted email.

I understand that there may be circumstances where I may be reappointed, referred to a private dentist, or denied treatment if it is determined that my obtaining treatment is not in my best interest or that of the Clinic.

I hereby certify that I am of legal age and responsible to accomplish this release, and have read and understand the Patient Bill of Rights above.

Witness________________________________________ Signature________________________________________

Patient, Parent, or Guardian

Date___________________________________________________
COURSE DIGITAL CAMERA POLICY for PATIENT PRIVACY

(There are three categories of safeguards: administrative, physical and technical)

Policy:

FSU Owned Digital Camera Use for Course Assignments:

Acceptable procedure for digital oral/intraoral imaging is with the use of the clinic digital camera, the Schick Intraoral camera and the Digi-Doc Intraoral camera - under the strict supervision of a clinical instructor.

Otherwise:

Staff and DH Student Duties - UNDER ALL CATEGORIES, PERSONAL PAGERS, CELL PHONES, PORTABLE COMPUTING DEVICES, AND/OR THEIR CAMERAS/VIDEOCAMERAS, PERSONAL COMPUTERS, PDA’S, BLACKBERRY’S, OR ANY OTHER PERSONAL ELECTRONIC EQUIPMENT IS NOT PERMITTED ON THE CLINIC FLOOR AND ARE PROHIBITED IN PATIENT TREATMENT LABS, CLINICAL SETTINGS AND THE DH COMPUTER LAB!

AUTHORIZED USERS: THERE ARE FEW INDIVIDUALS THAT MUST USE A CELL PHONE TO DO THEIR JOBS WHEN TROUBLE SHOOTING CLINICAL PROBLEMS; THOSE AUTHORIZED INDIVIDUALS WOULD BE: I.T. STAFF, DH CLINIC OPERATIONS SUPERVISOR, DH RADIOLOGY INSTRUCTOR, SUPERVISING DENTISTS, etc.

If a DH student needs to make a phone call to find a patient, etc., they may use the clinic land line telephone or excuse themselves from clinic, go to their locker and have the conversation with potential patients at the west end of the Health Professions building and away from the dental hygiene clinic. This safeguard will be strictly enforced. Professionalism Points may be deducted from a student’s lab or clinical grade if a violation should occur.

Work Study students that are working in the reception office area, the sterilization area are NOT authorized cell phone users and may not bring their cell phones or other electronic devices into the dental reception, clinical area. Violation of this safeguard will be strictly enforced and could result in termination.

Sharing any patient information in any form on social media such as Facebook, etc., is strictly prohibited.

Other sanctions will be determined by the Privacy Officer depending on the severity of the violation and will involve meeting with the Privacy Officer for further HIPAA training. If the violation is severe, further sanctions may involve the Department Head and/or FSU General Counsel.
All images captured with the FSU digital camera for course use that are emailed to the STUDENT will be completely de-identified.

Procedure:

PRIOR TO TAKING ORAL/INTRA ORAL PHOTOS THE FOLLOWING MUST OCCUR:

Student Duties:

1. Receive verbal consent from the patient and instructor to take oral/intra oral photos along with the written consent to treat in the Patient’s Bill of Rights/Consent form located & signed in the patient chart
2. Assemble armamentarium (e.g. cheek retractors and paddle mirrors as needed)
3. Indicate to instructor the oral/intra oral area to be photographed
4. Retract as needed
5. Document student name and most current & accurate email address (of student) on a sticky note and leave in the blue bin for emailing purposes (no patient names)
6. Students must document in services rendered “Oral photographs taken with patient consent”

Staff Duties (Clinical Instructors Only):

1. Acquire clinic digital camera from locked cabinet
2. Review verbal and written consent from patient before proceeding
3. Turn on camera
4. Select flower icon or flower icon in the box for oral/intra oral size photos (close-ups)
5. Take photos of the patients oral/intra oral features only
6. Use the zoom icons as needed
7. Press photo button half way down to focus
8. Once focused, press down all the way on the photo button to take the picture
9. After patient oral/intra oral photos are taken, take one more picture of the STUDENT, which separates patient photos on the camera
10. Record student name and current email address on a sticky note for emailing purposes
11. Return camera to locked cupboard after each clinic session
12. Confirm that the student has documented in services rendered in patient chart
Policy:

DOWNLOADING PHOTOS & EMAILING TO STUDENTS - ONLY TO BE DONE BY ASSIGNED COURSE INSTRUCTORS.

Procedure:

Staff Duties (Assigned Instructors):

1. Emailing of clinic oral/intra oral photos will take place each Friday
2. The instructor will gather all STUDENT email information and clinic camera
3. Connect camera to FSU computer via USB cord on assigned instructors office computers
4. Turn on camera
5. Access the “DCIM” file through the removable disk file and then select the individual camera files
6. Select photos to be emailed and delete all others not selected at this time
7. Send to STUDENT email recipient in medium size format (1024 x 768)
8. Once attached to the email through Lotus Notes type in the STUDENTS email address and in the body of the email state “Clinic Photos”
9. Patient names will not appear on any photos or in any area of the email (e.g. subject line, Cc; Bcc)
10. Only an image number e.g. IMG0339.jpg should appear in the body of the email and in the subject line.
11. All images are then deleted from the camera memory card
12. Return camera to locked cupboard in the main clinic area for future use in VFS 201
13. All sticky notes with student information is shredded

Clinic Digital Camera Management Policy

1. Only clinical instructors are authorized to use the clinic digital camera.
2. Regarding memory card disposal; when a memory card becomes nonfunctional the memory card will be shredded.
3. To ensure that images are not stored on the camera itself, as the camera ages and will no longer be in use, the FSU Dental Hygiene Department will give it to the FSU IT Department for destruction.

* F13 - FSU Dental Hygiene Clinic Camera Protocol Revision – St. Clair/Jackson
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

BREACH ASSESSMENT FORM

This form is to be used as a guide for the dental practice to assess suspected breaches of unsecured protected health information.

A. DESCRIBE THE INCIDENT:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Date the suspected breach was discovered?</td>
</tr>
<tr>
<td>2.</td>
<td>Date the suspected breach occurred?</td>
</tr>
<tr>
<td>3.</td>
<td>Describe with a brief statement of what happened.</td>
</tr>
<tr>
<td>4.</td>
<td>How we learned of the breach.</td>
</tr>
<tr>
<td>5.</td>
<td>Describe the people and entities involved.</td>
</tr>
<tr>
<td>6.</td>
<td>Did the incident involved “use” of information?</td>
</tr>
<tr>
<td>7.</td>
<td>Who used the information?</td>
</tr>
<tr>
<td>8.</td>
<td>For what purpose was the information used?</td>
</tr>
<tr>
<td>9.</td>
<td>If the incident involved a disclosure of information:</td>
</tr>
<tr>
<td>10.</td>
<td>Who disclosed the information?</td>
</tr>
<tr>
<td>11.</td>
<td>To whom?</td>
</tr>
<tr>
<td>12.</td>
<td>For what purpose?</td>
</tr>
<tr>
<td>13.</td>
<td>Describe the format of the information (paper chart, electronic, films)</td>
</tr>
<tr>
<td>14.</td>
<td>If electronic information was involved:</td>
</tr>
<tr>
<td>15.</td>
<td>Was the electronic information in storage? (On a desktop, computer hard drive, a laptop, a CD or a USB?)</td>
</tr>
<tr>
<td>16.</td>
<td>Was the electronic information in transit? (mail or through a portal?)</td>
</tr>
<tr>
<td>17.</td>
<td>Was the electronic information properly encrypted?</td>
</tr>
<tr>
<td>18.</td>
<td>Was the password of an authorized person/entity used to access the information?</td>
</tr>
</tbody>
</table>
19. What is being done to mitigate any risk to the privacy and security of the information?

**B. IF ANY OF THE FOLLOWING APPLY, HIPAA DOES NOT REQUIRE NOTIFICATION:**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Was the information properly “secured” using a method approved by the U.S. Dept. of HHS?</td>
<td>YES</td>
</tr>
<tr>
<td>2.</td>
<td>If YES, explain:</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Was the information PHI?</td>
<td>YES</td>
</tr>
<tr>
<td>4.</td>
<td>If NO, explain:</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Was the use or disclosure permitted or required? (Authorization forms required)</td>
<td>YES</td>
</tr>
<tr>
<td>6.</td>
<td>Attach a copy of the signed authorization form(s)</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Do any of the following EXCEPTIONS apply?</td>
<td></td>
</tr>
</tbody>
</table>

**Exception 1:**

- The incident involved unintentional acquisition, access or use of PHI by a workforce member, or by an individual or entity acting under the authority of the dental practice or one of its business associates,

- The acquisition, access or use was made:
  - In good faith, and
  - Within the scope of authority, and

- The acquisition, access or use does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

**EXCEPTION 2:**

The incident involved an inadvertent disclosure:

- By an individual or entity that is authorized to access PHI at the dental practice (or by one of its business associates)
- To another person authorized to access PHI at the dental practice (or the same business associate), and

- The information received as a result of such disclosure was not further used or disclosed in a manner not permitted under HIPAA Privacy Rule.

**EXCEPTION 3:**

The incident involved a disclosure of PHI, and

The dental practice or business associate (as applicable) has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

<table>
<thead>
<tr>
<th>Does any one of these three exceptions apply?</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>If YES, explain:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**C. RISK ASSESSMENT:**

If the information was unsecured PHI, and

- The use or disclosure was not permitted or required under HIPAA,

- The individual did not appropriately authorize the use or disclosure, and

- None of the above 3 exceptions apply,
then, the dental practice must send timely breach notification unless the dental practice demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of the relevant factors, including at least the following factors:

**FACTOR 1:** The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

**Assessment:**

**FACTOR 2:** The unauthorized person who used the protected health information or to whom the disclosure was made.

**Assessment:**

**FACTOR 3:** Whether the PHI was actually acquired or viewed.

**Assessment:**

**FACTOR 4:** The extent to which the risk to the PHI has been mitigated.

**Assessment:**

Should any additional relevant factors be considered in determining the probability that the PHI has been compromised? If so, describe below: (if more space is needed, attach another sheet of paper with explanation).

**Assessment:**

Based on a risk assessment involving all of the above factors, is there an overall low probability that the PHI has been compromised?

- The probability of compromise is LOW: __________
- The probability of compromise is HIGH: __________

**IF THE PROBABILITY THAT PHI HAS BEEN COMPROMISED IS NOT LOW, HIPAA BREACH NOTIFICATION IS REQUIRED! NOTIFY FSU GENERAL COUNSEL, IMMEDIATELY!**

Is notification required under other applicable federal, state or local law? YES/NO (Circle one)

If YES, explain:

This risk assessment form is accurate and complete.

Signed: __________________________________________ Date: ______________________

Name: _______________________________________________________________________________

Title: _______________________________________________________________________________ Date: _______________

Name: _______________________________________________________________________________

Title: _______________________________________________________________________________ Date: _______________
Breach Notification Policy

1. Breach Notification Team.

Ferris State University (“Ferris State”), a hybrid entity with health care components, has established a Breach Notification Team, which consists of the following members:

- Privacy Officer of the health care component where the violation may have occurred
- HIPAA Security Officer and member(s) of the Information Technology Services Security Incident Response Advisory Team, if applicable
- Vice President for Administration and Finance
- a representative from the General Counsel’s office

In the event of a potential breach of protected health information or “PHI” (as defined under HIPAA), Ferris State will investigate the incident consistent with its HIPAA Security Rule security incident procedures (if applicable). One or more members of the Breach Notification Team will participate in such investigation and report relevant facts to the Team for purposes of determining whether notification will be required.

In determining whether notification is required, the Breach Notification Team may consult with any additional employees, agents, contractors, consultants or other individuals reasonably necessary to determine whether Ferris State has a duty to notify individuals about a breach.

2. Investigation

In the event the Information Technology Department or a member of Ferris State’s workforce detects or otherwise learns of a security violation of its electronic or paper files, it will conduct an investigation of the security incident consistent with its Policies and Procedures. If the incident involves records containing PHI, the Information Technology Department will notify the Privacy Officer of the health care component where the violation may have occurred. Other workforce members who learn of an incident involving unauthorized access to PHI (whether in electronic or paper form) will also notify the Privacy Officer of the health care component where the violation may have occurred of the incident.
Upon notification of a potential incident of unauthorized access to PHI, the Privacy Officer of the health care component where the violation may have occurred will determine whether Ferris State has a duty to notify individuals about a breach. In determining whether notification is required, the Privacy Officer of the health care component where the violation may have occurred may consult with legal counsel, employees, agents, contractors or consultants as reasonably necessary to determine Ferris State’s notification obligations, if any.

3. **Determine whether a breach has occurred.**

The following are examples of the types of situations that may need evaluation. These include situations in which a contractor/business associate notifies Ferris State that an impermissible use or disclosure has or may have occurred:

- Ferris State learns that an unauthorized individual has gained access to Ferris State’s electronic information system.
- Ferris State learns that an authorized individual may have accessed protected health information for an improper purpose.
- Ferris State learns that information intended for an authorized individual was misdirected (for example, by e-mail or fax transmission).
- Ferris State learns that a business associate has suffered a potential data breach.
- Ferris State hears from individuals who are the subject of protected health information that they have been the victims of identity theft or other identity fraud crime.
- Ferris State learns that a client file that may contain sensitive information cannot be located.

If a situation requires evaluation, the Breach Notification Team should gather details about the incident, including the following:

- The specific data that is involved in the incident.
- Whether the access, use or disclosure is consistent with Ferris State’s HIPAA policies and procedures.
- The manner in which the information was accessed, used or disclosed, and the circumstances surrounding the incident.
- The date the incident was discovered.
- The date(s) the incident occurred.
- The number of individuals whose information was involved.
The states in which the individuals reside.

When Ferris State learns of a possible breach of either its electronic files or physical files the Breach Notification Team must first determine whether there has been an impermissible use or disclosure of unsecured protected health information under HIPAA’s Privacy Rule and/or whether the disclosure included confidential client information under the Michigan Rules of Professional Conduct.

If the facts indicate that the access, use, or disclosure was not permitted under HIPAA, the Breach Notification Team will need to determine whether the incident falls into one of the exceptions to the HIPAA breach notification requirements. Ferris State may not have a duty to notify if (A) the information is considered “secured”; (B) the incident is not considered a “breach”; or (C) the Protected Health Information has not been compromised, as described below.

Note: while much of this policy addresses breach notification requirements under HIPAA, most states have security breach notification requirements that may also apply. Therefore, the Breach Notification Team may need to consult with legal counsel to determine if Ferris State has any obligations under state notification laws—whether or not notification is required under HIPAA.

Note: in the event of a breach, Ferris State will also need to evaluate the effectiveness of its privacy and security practices and determine whether changes need to take place, consistent with Ferris State’s HIPAA evaluation procedures.

A. **Determine whether the information is deemed “secured” under HIPAA.**

The first step is to determine whether the information was properly secured under HIPAA. Whether the information is properly secured will depend on the nature of the information and how well it is protected.

- If the information is electronic, the data is considered secured if both of the following are true:
  1. The data has been properly encrypted consistent with guidance issued by the Department of Health & Human Services. This guidance may change from time to time, but as of September 2009, HHS guidance called for the following:
     - For data at rest (including data that resides in databases, file systems, flash drives, memory and other structured storage methods), the encryption process must be consistent with National Institute of Standards & Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*
For data in motion (which includes data moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange), the encryption process must comply, as appropriate, with one of the following:

- National Institute of Standards & Technology Special Publication 800-77, *Guide to IPsec VPNs*;
- National Institute of Standards & Technology Special Publication 800-113, *Guide to SSL VPNs*; or
- Other encryption processes that are Federal Information Processing Standards 140-2 validated.

2. The individual/entity with improper access to the information does not have access to the confidential decryption process or key.

- Data that has been destroyed may also be considered secured if one of the following is true:
  1. The information was stored on paper, film or other hard copy media, and the media has been shredded or destroyed in such a way that the protected health information cannot be reconstructed. (Note that redaction is not an effective form of destruction.)
  2. The information is in electronic form and has been cleared, purged or destroyed consistent with National Institute of Standards & Technology Special Publication 800-88, *Guidelines for Media Sanitization*, so that the protected health information cannot be retrieved.

If the information meets one of the tests above for being secured, the incident will not be considered a breach and notification will not be necessary.

If the Breach Notification Team concludes that the information is secured, it must document the facts leading to this conclusion. The Privacy Officer of the health care component where the violation may have occurred will make and retain the documentation for a period of at least six years from the date the Team concludes its evaluation of the incident.

B. **Determine whether the incident falls within an inadvertent acquisition or disclosure exception.**

If the information is not considered secured, the incident may still not be considered a breach if the incident falls within one of the following exceptions:
1. **Unintentional acquisition, access or use of protected health information.**
   In order for this exception to apply, all of the following have to be true:
   
   a. the unauthorized acquisition, access or use of protected health information must have been unintentional;
   
   b. the individual who acquired, accessed or used the protected health information must be one of the following:
      
      • a member of Ferris State’s workforce
      • A member of a business associate’s workforce
      • A person acting under the authority of Ferris State or Ferris State’s business associate
   
   c. The individual who acquired, accessed or used the protected health information did so in good faith.
   
   d. The acquisition, access or use did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

2. **Inadvertent internal disclosure of protected health information.** This exception applies if all of the following are true:
   
   a. The disclosure is made by an individual who is authorized to access protected health information
   
   b. The disclosure is made to an individual who is authorized to access protected health information.
   
   c. Both individuals work for the same organization, which may be one of the following:
      
      • Ferris State
      • Ferris State’s business associate
      • An organized health care arrangement in which Ferris State participates.
   
   d. The disclosure did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

3. **Where the information would not be retained.** This exception applies if all of the following are true:
   
   a. The disclosure is made to an unauthorized individual.
b. Ferris State or its business associate has a good-faith belief that the unauthorized individual would not reasonably have been able to retain the information.

If the Breach Notification Team concludes that the incident meets one of the exception tests above, the incident will not be considered a breach and notification will not be necessary. The Team must document its analysis leading to this conclusion. The documentation must be retained for a period of at least six years from the date the Team concludes its evaluation of the incident.

C. **Determine the probability that the Protected Health Information has been compromised.**

If the Breach Notification Team determines that the information did not meet the requirements for being secured or fall within one of the exceptions noted above, the Team must conduct a risk assessment. There is a presumption that an impermissible use or disclosure is a breach unless it can be determined through a risk assessment that there is a low probability that the Protected Health Information has been compromised.

Factors to consider include:

- The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification.
  - Did it include social security numbers, driver’s license numbers, bank account/credit card numbers, insurance numbers, or other sensitive information that could be used for identity theft or identity fraud crimes?
  - Did it include information about medical treatment, diagnoses, diseases, or similar details about an individual’s health?
  - What is the likelihood that the Protected Health Information could be reidentified based on the context and the ability to link the information with other available information?
- The unauthorized person who used the Protected Health Information or to whom the disclosure was made.
  - Was the recipient also a HIPAA covered entity with a legal duty not to misuse the information?
  - Does the recipient have a contractual relationship with Ferris State that prohibits it from misusing the information?
  - Are there other facts and circumstances that would indicate that the recipient of the information is unlikely to misuse the information?
- Whether the Protected Health Information was actually acquired or viewed.
  - Does a forensic analysis indicate that Protected Health Information on a lost computer was never accessed, viewed, acquired, transferred or otherwise compromised?
- The extent to which the risk to the PHI has been mitigated.
• Are there past dealings with the recipient or other factors that would indicate that the recipient can be trusted not to use or further disclose the information?

The Breach Notification Team should consider these and other pertinent facts to determine whether there is a low probability that the Protected Health Information has been compromised.

If the Breach Notification Team concludes that there is a low probability that the Protected Health Information has been compromised, then notification is not required. The Team must document its analysis leading to this conclusion and retain this documentation for at least six years from the date the Team concludes its evaluation of the incident.

4. Special considerations for breaches involving Business Associates (or for business associates, subcontractors)

Under HIPAA, a business associate who maintains protected health information on behalf of Ferris State has a duty to notify Ferris State of the breach within 60 days, but it is Ferris State’s duty to provide notification to the individuals impacted by the breach. Moreover, in certain circumstances, Ferris State may be charged with the business associate’s knowledge of the breach, so that the deadline for providing notice will be based upon when the business associate knew or should have known about the breach.

In order to reduce the risk to Ferris State of a HIPAA violation, Ferris State will seek to include in its business associate agreements a provision that requires the business associate to notify Ferris State of a potential breach within 5 business days of discovery and to provide information about the individuals involved in the potential breach within 30 days of discovery. When appropriate, and after reaching consensus with business associate, Ferris State may also include a provision in the business associate agreement allocating responsibility for notification between Ferris State and business associate. When a business associate reports a potential breach to Ferris State, the Breach Notification Team will work with the business associate to determine whether the incident requires notification.

5. Notification

If the Breach Notification Team determines that Ferris State must provide notification of the incident, the Team will prepare appropriate notification as required below.

A. Notice to Individuals

Under HIPAA, Ferris State must provide notice to affected individuals without unreasonable delay, but no later than 60 days after the date Ferris State discovers the breach or should have discovered the breach if it had exercised appropriate diligence. In order to reduce
the risk of exceeding the deadline, Ferris State will seek to provide notice as soon as reasonably possible once it has discovered the breach.

The HIPAA breach notification regulations require that the following information be included in the notification:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach.
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what Ferris State is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.

All notifications must be written in plain language.

Notice may be provided by e-mail to individuals who have agreed in advance to receive electronic notice. Otherwise, notice must be sent via first class mail. If Ferris State knows that an individual is deceased and has the address of the deceased’s next of kin or personal representative, Ferris State may send the written notification to either next of kin or the personal representative.

Under HIPAA, Ferris State has no more than 60 days after discovery of the disclosure to notify individuals. The date of discovery is measured as follows:

- First day the breach is known to a member of the Ferris State’s workforce or agents;
  - workforce member includes any employee, partner, volunteer, trainee, agent, etc.

- First day a member of the Ferris State workforce or its agents would have known of the breach by exercising reasonable diligence; or

- First day that Ferris State is notified of a breach by any of its independent contractors (unless the independent contractor is deemed to be an agent).

Note: State security breach notification laws may also apply and may mandate a shorter time frame for notification.
If Ferris State does not have sufficient contact information for some or all of the affected individuals (or if the contact information is outdated) then Ferris State must provide substitute notice for such individuals in the following manner:

- If fewer than 10 individuals are affected, substitute notice can be provided to these individuals via telephone or other written notice that is reasonably calculated to reach the individuals.

- If more than 10 individuals are affected, HIPAA requires the following:
  
  - a conspicuous posting for a period of 90 days on Ferris State’s home page or a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside; and
  
  - a toll-free phone number active for 90 days where an individual can learn whether the individual’s unsecured protected health information may be included in the breach.

- The content of the substitute notice must include all of the elements required for the standard notice described above.

- Substitute notice is not required in situations where an individual is deceased and Ferris State does not have sufficient contact information for the deceased individual’s next of kin or personal representative.

If Ferris State believes that there is the possibility of imminent misuse of unsecured protected health information Ferris State may also provide expedited notice by telephone or other means. This notice is in addition to, and not in lieu of, direct written notice.

Ferris State must retain copies of all notifications for at least six years from the date the notifications were provided. For substitute notifications, retain copies for at least six years from the date the notification was last posted on the website or the date the notification last ran in print or broadcast media.

**B. Notice to the Media**

If the Breach Notification Team determines that notification is required to more than 500 residents of a state, Ferris State must provide notice in the form of a press release to prominent media outlets serving the state. The press release must include the same information required in the written notice provided to individuals. The Breach Notification Team may coordinate such notice with Ferris State’s public relations department or other public relations consultants, as appropriate.

**Note:** State security breach notification laws should also be consulted to determine whether there are additional notification obligations to the media, state agencies, or national credit bureaus.
Ferris State must retain copies of all press releases provided to prominent media outlets for at least six years from the date the notifications were provided.

C. To the Department of Health & Human Services

If the Breach Notification Team determines that Ferris State or its business associate must provide notification to individuals under HPAA, then Ferris State will also have to provide notification to the Department of Health & Human Services. The timing of the notification will depend on the number of individuals affected by the incident:

- If the breach involves more than 500 individuals (regardless of whether they reside in the same state or in multiple states), Ferris State will notify the Department of Health & Human Services without unreasonable delay, but no later than 60 days after discovery. This notification is to be submitted to the Department of Health & Human Services contemporaneously with the written notifications sent to individuals and in the manner specified on the Department’s Web site.

- If the breach involves fewer than 500 individuals:
  
  o The Privacy Officer of the health care component where the violation may have occurred must maintain a log of notifications involving fewer than 500 individuals. The information to be recorded in the log will be set forth on the Department of Health & Human Services’ Web site.
  
  o The Privacy Officer of the health care component where the violation may have occurred, in coordination and consultation with the General Counsel’s Office, will submit the log to the Department of Health & Human Services for each calendar year by February 28 of the following year, in the manner specified on the Department’s Web site.

Notifications to the Department of Health & Human Services, including the annual log of notifications, must be maintained for at least six years from the date submitted to the Department.

6. Notification (For use when Ferris State is considered a Business Associate)

If Ferris State discovers a potential breach, the Breach Notification Team will review the business associate agreement with the covered entity or entities whose data is involved in the incident and, if addressed in the business associate agreement, will follow the requirements set forth in the agreement.

To the extent not addressed in the business associate agreement, Ferris State will use the following default rules set forth in HIPAA:
• Ferris State will notify the covered entity as soon as possible after discovering a potential breach, and no later than 60 days after discovery.

• Ferris State will provide the covered entity with the following information, either at the time Ferris State provides notice of the potential breach to the covered entity or promptly thereafter as the information becomes available:
  
  o The identity of each individual whose unsecured protected health information has been, or is reasonably believed to have been, breached, to the extent possible.

  o Any other available information that the covered entity is required to include in the notification to the individual. This may include the following:

    ▪ A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

    ▪ A description of the types of unsecured protected health information that were involved in the breach.

    ▪ Any steps the individual should take to protect themselves from potential harm resulting from the breach.

    ▪ A brief description of what Ferris State is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

    ▪ Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.

• Ferris State will cooperate with covered entity in determining whether notification is required under HIPAA.
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

BREACH LOG FORM

This form documents how our dental practice logs breaches that affect less than 500 individuals for annual submission to the U.S. Department of Health and Human Services (HHS).

Date of breach: ______________________________________________________________

Date breach was discovered: ____________________________________________________________

Did the breach occur at or by a business associate?

☐ YES

☐ NO

If YES:

Name of business associate: ______________________________________________________

Address: _____________________________________________________________________________

City: __________________________________ State: ___________________ Zip code: ______________

Business associate contact name: ______________________________________________________

Business associate contact phone number: __________________________________________________

Business associate contact email: _______________________________________________________

Approximate number of individuals affected by the breach: _________________________________

Type of breach:

☐ Theft

☐ Loss

☐ Improper disposal

☐ Unauthorized access or disclosure

☐ Hacking or information technology incident

☐ Unknown

☐ Other: _____________________________________________________________________________

Where was the breached information located?
Laptop
Desktop computer
Network server
Email
Other portable electronic device
Other
Electronic medical record
Paper

Type of patient information involved:

Demographic Information
  - Name
  - Social Security number
  - Address or zip code
  - Date of birth
  - Other identifier

Financial Information
  - Bank account information
  - Claims information
  - Other financial information

Clinical Information
  - Diagnosis or conditions
  - Lab results
  - Medications
  - Other treatment information

Other

Brief Description of the breach (include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach). May need to use another sheet of paper and attach.

What safeguards (protective measures) were in place prior to the breach?

Firewalls
Packet filtering (router-based)
Secure browser sessions
Strong authentication
Encrypted wireless
Physical security
Logical access control
☐ Anti-virus software
☐ Intrusion detection
☐ Biometrics

Date(s) notice was provided to affected individuals:

Date first notice was sent:

Month: ____________________ Day: _____________ Year: ______________________

Date last notice was sent:

Month: ____________________ Day: _____________ Year: ______________________

Was substitute notice required? (Substitute notice is required if you lack sufficient or up to date contact information for any affected individuals)

☐ YES
☐ NO

Was media notice required? (Medial notice is required if a breach involves 501 or more residents of a state or jurisdiction)

☐ YES
☐ NO

What action did the dental practice take in response to the breach?

☐ Security and/or privacy safeguards
☐ Mitigation (actions to lessen the harm of the breach to the affected individuals)
☐ Sanctions (against workforce members who violated the policies and procedures)
☐ Policies and procedures
☐ Other

If other, please describe:
Describe in detail any additional actions taken following the breach:
AGREEMENT TO RECEIVE ELECTRONIC COMMUNICATION

This form documents how our dental practice obtains patient agreement to receive communications via email.

Patient Name: __________________________________________ Date of Birth: ______________________

I agree that the Ferris State University Dental Hygiene Clinic and/or Ferris State University General Counsel may communicate with me electronically at the email address below.

I am aware that there is some level of risk that third parties might be able to read unencrypted emails.

I am responsible for providing the dental practice any updates to my email address.

I can withdraw my consent to electronic emails by calling:

FSU Dental Hygiene Clinic: 231-591-2260. The office will notify the Privacy Officer of any changes to this agreement.

Email Address (PLEASE PRINT CLEARLY):

___________________________________________________@________________________________

Patient Signature: __________________________________ Date: __________________________
This form documents the complaints regarding the dental practice’s privacy practices or HIPAA compliance.

<table>
<thead>
<tr>
<th>Complaint</th>
<th>Name and contact information of the person making the complaint</th>
<th>Date complaint was made</th>
<th>Date response sent to person who made the complaint</th>
<th>Sanctions, if any</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Describe any changes resulting from the complaint, i.e., training, Policy and Procedure redesign:
Clinic section notebooks are to be used to record anecdotal student observations and comments related to clinic progress and presentation only. The purpose of these notes is to monitor student progress and document observations and progress that are not otherwise demonstrated through clinical assessments. These shall serve as records which will support a student’s progression or non-progression to the next clinical academic semester.

These notebooks shall not be used for patient information at any time. Patient information is to remain in their individual charts alone. At no time should patient names be recorded or referenced within these notes.

The notebooks and contents of the notes shall be kept locked in a clinic cabinet previously designated for this purpose, accessible to instructors only. At the end of the two year dental hygiene program, once students have successfully graduated, all student clinical anecdotal records will be shredded.

This memo is to serve as notification to all affected parties and will remain first year clinic policy until further notice.
All student tracking forms and student clinic grade sheets will be housed in a section notebook. This notebook will not leave the clinical area during the active semester that the student is in the course/clinic and will be stored in a locked cabinet.

Within the notebook the following items will be housed for each student (by semester):

- Tutoring forms for the student
- Tracking forms (accreditation requested)
- Clinical tests
- Completed patient performance forms (yellow copy)
- Completed observations or process evaluations
- Notes, as needed
- Professionalism Forms

All radiographic grade forms will be stored in VFS 203 (instructor’s room) in a file cabinet and will not leave the clinical area, as well. This room will be locked when the instructor is not in the area.

Once a semester is completed, all student records will go into a file created specifically for that student and will be stored in VFS 205 in a locked file cabinet until one year after the student has graduated. At that time, the forms will be shredded using the University’s shredding company.
INTEROFFICE MEMORANDUM

To: Cameo McGowen, Becky Walsh-Zimmerman, and office work study students
From: Annette Jackson, DH Clinic Operations Supervisor
Re: PATIENT PRIVACY and MANAGEMENT OF STUDENT PERFORMANCE FORMS and BILLING RECORDS
Date: December 2, 2013

As of this date, I will request that for patient privacy reasons (HIPAA) that the file cabinets in VFS 202 that hold the student’s Performance Forms and all Billing forms be locked at all times when not in use.

Doing this will be one of the physical safeguards that we can do to ensure the safety and privacy of patient information.

If you need appropriate keys, please let me know, but I believe we should be all set with the appropriate keys for these file cabinets. Please advise all staff working in the office about this change.
FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA

STUDENT PERFORMANCE FORMS FOR DH CLINIC (EXAMPLES)

The following forms serve as examples demonstrating how clinic course instructors manage patient names and the dates of the patient appointments on the student clinic grade sheet. These forms are created using NCR paper. The original goes into our file (programmatic) and is securely stored for 1 year after the student graduates. The copy goes to the student and is maintained within the clinical setting. After the appropriate time, all forms will be shredded using the FSU Shredding Service that we are contracted with. All clinic forms that deal with patient treatment will not leave the clinical area at any time.
### FERRIS STATE UNIVERSITY
**DENTAL HYGIENE PROGRAM – STUDENT PERFORMANCE FORM—DHYG 126**

<table>
<thead>
<tr>
<th>General Evaluation Points:</th>
<th>Inst. Initials</th>
<th>Calculus Detection</th>
<th>Calculus Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical History</td>
<td>5/3/0</td>
<td>Student</td>
<td>0 = No calculus</td>
</tr>
<tr>
<td>Intra/Extra Oral Exam</td>
<td>10/5/0</td>
<td>3</td>
<td>1 = Light calculus</td>
</tr>
<tr>
<td>Hard Tissue Charting</td>
<td>5/3/0</td>
<td>9</td>
<td>2 = Moderate calculus</td>
</tr>
<tr>
<td>PSR Assessment</td>
<td>8/4/0</td>
<td>14</td>
<td>3 = Heavy calculus</td>
</tr>
<tr>
<td>Case Type</td>
<td>2/1/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Education</td>
<td>5/3/0</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Chain of Asepsis</td>
<td>10/5/0</td>
<td>25/p</td>
<td></td>
</tr>
<tr>
<td>Documentation</td>
<td>5/3/0</td>
<td>29/t</td>
<td></td>
</tr>
</tbody>
</table>

**Calculus Level**

\[
\text{Total} \div 6 = \text{Average}\]

\[
\text{Multiply total number of teeth in dentition} = \text{Calculus level}\]

<table>
<thead>
<tr>
<th>Patient Completed: Errors Noted*</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 ___ #9/f ___ #17 ___ #25/p ___</td>
</tr>
<tr>
<td>#2 ___ #10/g ___ #18 ___ #26/q ___</td>
</tr>
<tr>
<td>#3 ___ #11/h ___ #19 ___ #27/r ___</td>
</tr>
<tr>
<td>#4/a ___ #12/i ___ #20/k ___ #28/s ___</td>
</tr>
<tr>
<td>#5/b ___ #13/j ___ #21/l ___ #29/t ___</td>
</tr>
<tr>
<td>#6/c ___ #14 ___ #22/m ___ #30 ___</td>
</tr>
<tr>
<td>#7/d ___ #15 ___ #23/n ___ #31 ___</td>
</tr>
<tr>
<td>#8/e ___ #16 ___ #24/o ___ #32 ___</td>
</tr>
</tbody>
</table>

**Error Legend**

- P = Plaque
- T = Tissue Trauma
- C = Calculus
- S = Stain

**Time Goal:** __________    **Actual Time:** __________

**Time Goal is for student feedback only.**

1 = **Light (L)** Calculus – fine, granular, grainy, located along line angles, marginal areas, and/or under contacts. Slight vibration or roughness detected with explorer. (Sandpaper)

2 = **Moderate (M)** Calculus – a bump with thickness readily discernible, a marginal ring or interproximal “click” with explorer, definite vibration felt with explorer a “jump”.

3 = **Heavy (H)** Calculus – ledge encircling tooth or a portion of tooth, thick and dense fills interproximal space or is a marginal ledge, definite large "bump", sometimes “binds” explorer.

**Total number of errors__ x Semester 1 = (Adjusted Error Total)**

<table>
<thead>
<tr>
<th>Semester: DHYG 126 = 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Semester: DHYG 215 = 2</td>
</tr>
<tr>
<td>Semester: DHYG 225 = 3</td>
</tr>
</tbody>
</table>

**Comments:**

**Recommended Recall Frequency**

<table>
<thead>
<tr>
<th>Month</th>
<th>Year</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Medical Alerts</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Appointment</th>
<th>One</th>
<th>Two</th>
<th>Three</th>
<th>Four</th>
<th>Five</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finish Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instructor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Student Performance Form Instructions

The student must have a medical history check in with the section instructor before proceeding with the evaluation. Calculus detection will be on designated teeth, if a patient is missing one of the designated teeth, cross off the assigned tooth and insert an adjacent tooth. Example: if #3 is missing select #2.

The legend provides the level of calculus present on the tooth. The level will identify calculus on all surfaces of the tooth. Example: a tooth could have level 3 (heavy) calculus on the buccal surface and level 0 (no) calculus on the lingual, the student would then mentally average the calculus decide the entire tooth was a level 2 (moderate) calculus for the final evaluation.

To assess points in the General Evaluation Section use the following criteria.

<table>
<thead>
<tr>
<th>Evaluation area</th>
<th>Errors</th>
<th>Points Awarded</th>
<th>Documentation</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical History</td>
<td>None</td>
<td>5</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
<tr>
<td>Medical History</td>
<td>One Error</td>
<td>3</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
<tr>
<td>Medical History</td>
<td>Two Errors or more</td>
<td>0</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
</tbody>
</table>

To determine the calculus level, total the numbers assigned for calculus detection on each of the six teeth evaluated. Once a total number has been added, that total is then divided by 6 (the number of the teeth evaluated for calculus.) To get a calculus detection level, multiple the total number of teeth the patient has by the calculus average.

**Calculus Detection** (Example)

<table>
<thead>
<tr>
<th>Student</th>
<th>Faculty</th>
</tr>
</thead>
<tbody>
<tr>
<td>#3</td>
<td>2</td>
</tr>
<tr>
<td>#9</td>
<td>0</td>
</tr>
<tr>
<td>#14</td>
<td>1</td>
</tr>
<tr>
<td>#19</td>
<td>2</td>
</tr>
<tr>
<td>#25</td>
<td>2</td>
</tr>
<tr>
<td>#29</td>
<td>2</td>
</tr>
</tbody>
</table>

**Note:** The lines adjacent to the tooth numbers the student identified calculus on is blank. The blank signifies the instructor agreed with the calculus detection evaluation of the student.

If the instructor disagrees with the student calculus level the instructor would insert a different number next to the student’s calculus level.

Multiple by number of teeth in dentition = 28

Calculus detector: 160

Total 10 = 6 = Calculus Average 1.66

28 x 1.66 = 46.88

Equals Calculus level 46.48

**Calculus, Plaque, Stain Removal Evaluation**

After the student has completed the scaling and debridement a final evaluation is done. Next to each tooth is a blank that will contain the code if errors are noted calculus, plaque/stain and or tissue trauma is present after the instructor check. After the instructor has checked the dentition, an example of how the results could be is as follows: #3 P.C.T indicating that the instructor found plaque/stain, calculus and tissue trauma on #3 , plaque on #18 and calculus on #26. The total number of errors is 5. Refer to the example on the other side of this page under the title Calculus Removal Evaluation.

**Adjusted Error Total Calculation**

To calculate the adjusted error total, the total errors noted under the Final Evaluation section is added together. The total errors is documented in the Total number of errors blank and then multiplied by the semester (which is 1 for DHYG 125, 2 for DHYG 215, and 3 for DHYG 225). The difficulty level increases with each semester.

Refer to the example on the other side of this page under the title Total number of errors.

Total # of Errors ___5___ multiplied by Semester = 1

Adjusted Error total = 5

**Final Score Calculation**

You must now calculate the total General Evaluation Points at the top left of the page. Complete areas that were not previously evaluated and total the points the student received. Example: the score was 42/50

Calculus Detection Level 46.48 + General Evaluation Points (50) = Total Point Value 96.48

Subtract General Evaluation Errors + Adjusted Error Total = 12

7 + 5 = 12

Adjusted Error Total - Total Point Value = 84.48

12 – 96.48 = 84.48

Final Points = Total Point Value = Final Points 87.5
**FERMIS STATE UNIVERSITY**  
**DENTAL HYGIENE PROGRAM – STUDENT PERFORMANCE FORM—DHYG 126**

**Student:**

<table>
<thead>
<tr>
<th>General Evaluation Points</th>
<th>Inst. Initials</th>
<th>Calculus Detection</th>
<th>Calculus Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical History</td>
<td>5/3/0</td>
<td>Student</td>
<td>0 = No calculus</td>
</tr>
<tr>
<td>Intra/Extra Oral Exam</td>
<td>10/5/0</td>
<td>#3</td>
<td>1 = Light calculus</td>
</tr>
<tr>
<td>Hard Tissue Charting</td>
<td>5/3/0</td>
<td>#9/f</td>
<td>2 = Moderate calculus</td>
</tr>
<tr>
<td>PSR Assessment</td>
<td>8/4/0</td>
<td>#14</td>
<td>3 = Heavy calculus</td>
</tr>
<tr>
<td>Case Type</td>
<td>2/1/0</td>
<td>#19</td>
<td></td>
</tr>
<tr>
<td>Patient Education</td>
<td>5/3/0</td>
<td>#25/p</td>
<td></td>
</tr>
<tr>
<td>Chain of Asepsis</td>
<td>10/5/0</td>
<td>#29/t</td>
<td></td>
</tr>
<tr>
<td>Documentation</td>
<td>5/3/0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total: __________/50

**General Evaluation Errors**  
(If child patient, give 8 points for PSR Assessment)  
*Pt. type: child 0-9 yrs. adult adolescent 10-18 yrs.*

**Patient Completed: Errors Noted***

| #1 | #9/f | #17 | #25/p |
| #2 | #10/g | #18 | #26/q |
| #3 | #11/h | #19 | #27/r |
| #4/a | #12/j | #20/k | #28/s |
| #5/b | #13/j | #21/l | #29/t |
| #6/c | #14 | #22/m | #30 |
| #7/d | #15 | #23/n | #31 |
| #8/e | #16 | #24/o | #32 |

Total number of errors _______ x Semester(1) = _______  
(Adjusted Error Total)

Semester: DHYG 126 = 1  
Semester: DHYG 215 = 2  
Semester: DHYG 225 = 3

Calculus Level + General Evaluation Points (50) = Total Point Value  
Subtract (General Evaluation Errors + Adjusted Error Total)  

**Final Points**  

| Medical Alerts | 
|----------------|----------------|

**Recommended Recall Frequency**  
Month__________ Year__________

**Appointment**  
<table>
<thead>
<tr>
<th>One</th>
<th>Two</th>
<th>Three</th>
<th>Four</th>
<th>Five</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Finish Time</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Instructor**
Student Performance Form Instructions

The student must have a medical history check in with the section instructor before proceeding with the evaluation. Calculus detection will be on designated teeth, if a patient is missing one of the designated teeth, cross off the assigned tooth and insert an adjacent tooth. Example: if #3 is missing select #2.

The legend provides the level of calculus present on the tooth. The level will identify calculus on all surfaces of the tooth. Example: a tooth could have level 3 (heavy) calculus on the buccal surface and level 0 (no) calculus on the lingual, the student would then mentally average the calculus decide the entire tooth was a level 2 (moderate) calculus for the final evaluation.

To assess points in the General Evaluation Section use the following criteria.

<table>
<thead>
<tr>
<th>Evaluation area</th>
<th>Errors</th>
<th>Points Awarded</th>
<th>Documentation</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical History None</td>
<td>0</td>
<td>5</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
<tr>
<td>Medical History One Error</td>
<td>1</td>
<td>3</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
<tr>
<td>Medical History Two Errors or more</td>
<td>2</td>
<td>0</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
</tbody>
</table>

To determine the calculus level, total the numbers assigned for calculus detection on each of the six teeth evaluated. Once a total number has been added, that total is then divided by 6 (the number of the teeth evaluated for calculus.) To get a calculus detection level, multiple the total number of teeth the patient has by the calculus average.

**Calculus Detection (Example)**

<table>
<thead>
<tr>
<th>Student</th>
<th>Faculty</th>
<th>Note: The lines adjacent to the tooth numbers the student identified calculus on is blank. The blank signifies the instructor agreed with the calculus detection evaluation of the student.</th>
</tr>
</thead>
<tbody>
<tr>
<td>#3</td>
<td>2</td>
<td>If the instructor disagrees with the student calculus level the instructor would insert a different number next to the student calculus level.</td>
</tr>
<tr>
<td>#9</td>
<td>0</td>
<td>28 x 1.66 = 46.48</td>
</tr>
<tr>
<td>#14</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>#19</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>#25</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>#26</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Multiple by number of teeth in dentition = 28

**Calculus, Plaque, Stain Removal Evaluation**

After the student has completed the scaling and or scaling and polishing a final evaluation is done. Next to each tooth is a blank that will ONLY have items from the legend on it if errors are noted (calculus, plaque/stain, or tissue trauma is present) after the instructor check. After the instructor has checked the dentition, an example of how the results could be is as follows: #3 P,C,T, indicating that the instructor found plaque/stain, calculus and tissue trauma on #3. Plaque on #18 and calculus on #25. The total number of errors is 5. Refer to the example on the other side of this page under the title Calculus Removal Evaluation.

**Adjusted Error Total Calculation**

To calculate the adjusted error total, the total errors noted under the Final Evaluation section is added together. The total errors is documented in the Total number of errors blank and then multiplied by the semester (which is 1 for DHYG 125, 2 for DHYG 215, and 3 for DHYG 225). The difficulty level increases with each semester.

Refer to the example on the other side of this page under the title Total number of errors.

Total # of Errors _5_ multiplied by Semester = 1

Adjusted Error total = 5

**Final Score Calculation**

You must now calculate the total General Evaluation Points at the top left of the page. Complete areas that were not previously evaluated and total the points the student received. Example: the score was 42/50

Calculus Detection Level 46.48 + General Evaluation Points (50) = Total Point Value 96.48

Subtract General Evaluation Errors + Adjusted Error Total = 12

Adjusted Error Total - Total Point Value = 84.48

Final Points - Total Point Value = Final Points 87.5
FSU DENTAL HYGIENE PROGRAM
DHYG 233 STUDENT PERFORMANCE FORM

Student: ____________________________

Patient: ____________________________ Patient Case Type: ______________

Periodontal Disease: Chronic-G__ Chronic-L__ Aggressive-G__ Aggressive-L__ Active__ Inactive__ Other__

Medically Compromised: ______ Geriatric (65 & up): ______ Special Needs: ______ Adolescent (12-18): ______

General Evaluation Points: ____________________________

<table>
<thead>
<tr>
<th>Medical History/ASA Class</th>
<th>Instr.</th>
<th>Initials</th>
<th>Calculus Detection</th>
<th>Calculus Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/3/0</td>
<td>#</td>
<td></td>
<td>Student</td>
<td>0 = No calculus</td>
</tr>
<tr>
<td>5/3/0</td>
<td>#</td>
<td></td>
<td>Faculty</td>
<td>1 = Light calculus</td>
</tr>
<tr>
<td>10/5/0</td>
<td>#</td>
<td></td>
<td>#14</td>
<td>2/3 = Mod/heavy calculus</td>
</tr>
<tr>
<td>10/5/0</td>
<td>#</td>
<td></td>
<td>#19</td>
<td>(or &quot;board&quot; calculus)</td>
</tr>
<tr>
<td>5/3/0</td>
<td>#</td>
<td></td>
<td>#24</td>
<td>*Errors:________</td>
</tr>
<tr>
<td>5/3/0</td>
<td>#</td>
<td></td>
<td>#25</td>
<td>0=10, 1=5, 4=6</td>
</tr>
<tr>
<td>5/3/0</td>
<td>#</td>
<td></td>
<td>*Corresponding errors:________</td>
<td></td>
</tr>
</tbody>
</table>

Time Management (use form) 5/3/0 ______

Time goal after check-in ______ Actual time ______

Instructor Feedback: ____________________________________________________________

Total (faculty) ______ + 6 = Avg. ______ X ______

Total number of teeth in dentition ______ = ______

Debridement Complete: Errors

| #1 | F#9 | #17 | P#25 |
| #2 | G#10 | #18 | Q#26 |
| #3 | H#11 | #19 | R#27 |
| A#4 | I#12 | K#20 | S#28 |
| B#5 | J#13 | L#21 | T#29 |
| C#6 | #14 | M#22 | #30 |
| D#7 | #15 | N#23 | #31 |
| E#8 | #16 | O#24 | #32 |

Calculus Level 1 = Light (L) Calculus — fine, granular, grainy, located along line angles, marginal areas, and/or under contacts. Slight vibration or roughness detected with explorer.

2 = Moderate (M) Calculus — a bump with thickness readily discernible, a marginal ring or interproximal "click" with explorer, definite vibration felt with explorer, a "jump."

3 = Heavy (H) Calculus — ledge encircling tooth, thick and dense fills interproximal space or is a marginal ledge, definite vibration, sometimes "binds" explorer.

Debridement Error Legend: C = Calculus P = Plaque S = Stain T = Tissue Trauma

Total # of errors ______ x Semester 3 = ______ Adjusted Error Total

Semester: DHYG 126 = 1
Semester: DHYG 224 = 2

Instr.Intials Semester: DHYG 233 = 3

Calcium Level + General Evaluation Points 50 = Total Point Value
Subtract (General Evaluation Errors Adjusted Error Total) = ______

Final Points + Total Point Value = ______ %

Comments: ____________________________

Medical Alerts: ____________________________

Recommended Recare Frequency: ____________________________

Month ______ Year ______

<table>
<thead>
<tr>
<th>Appointment</th>
<th>One</th>
<th>Two</th>
<th>Three</th>
<th>Four</th>
<th>Five</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finish Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instructor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Student Performance Form Instructions

The student must have a medical history check in with the section instructor before proceeding with the evaluation.
To assess points in the General Evaluation Section use the following criteria.
The instructor should give the student a time goal in DHYG 225 to help the student become more efficient and to be able to
adapt to the office setting. Please refer to the manual form "Student Time Management in Clinic."

| Example |
|------------------|------------------|------------------|------------------|
| Evaluation area  | Errors | Points Awarded | Documentation | Signature |
| Medical History  | None   | 5              | Circle points received | Instructor initials |
| Medical History  | One Error | 3              | Circle points received | Instructor initials |
| Medical History  | Two Errors or more | 0              | Circle points received | Instructor initials |

Calculus detection will be on designated teeth, if a patient is missing one of the designated teeth, cross off the assigned tooth
and insert an adjacent tooth. Example: if #3 is missing select #2. The legend provides the level of calculus present on the

tooth.

To determine the calculus level, total the numbers assigned for calculus detection on each of the six teeth evaluated. Once a
total number has been added, that total is then divided by 6 (the number of the teeth evaluated for calculus.) To get a
calculus detection level, multiple the total number of teeth the patient has by the calculus average.

**Calculus Detection (Example)**

<table>
<thead>
<tr>
<th>Student</th>
<th>Faculty</th>
<th>Note: The student identifies calculus level and records in the blanks</th>
</tr>
</thead>
<tbody>
<tr>
<td>#3</td>
<td>2</td>
<td>If the instructor then identifies calculus level and records in blanks,</td>
</tr>
<tr>
<td>#9</td>
<td>1</td>
<td>whether or not if it is the same number as the student’s.</td>
</tr>
<tr>
<td>#14</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>#19</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>#30</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Total 5 + 6 = Calculus Average .83

Multiple by number of teeth in dentition = 28
28 x .83 = 23.24
Equals Calculus level 23.24

Since there are 3 calculus detection errors, the student would receive 3 points for Calculus Detection under General
Evaluation Points. Calculus Detection will be graded as follows: 0-1 errors=10 points, 2-3 errors=5, and 4-6 errors=0
points

**Calculus, Plaque, Stain Removal Evaluation**

After the student has completed the scaling/and or scaling and polishing a final evaluation is done. Next to each tooth is a
blank that will ONLY have items from the legend on it if errors are noted (calculus, plaque/stain and or tissue trauma is
present) after the instructor check. After the instructor has checked the dentition, an example of how the results could be is
as follows: #3 P,C,T, indicating that the instructor found plaque/stain, calculus and tissue trauma on #3, #18 P and #25 C.
The total number of errors is 5.

**Adjusted Error Total Calculation**

To calculate the adjusted error total, the total errors noted under the Final Evaluation section is added together. The total
errors is documented in the Total number of errors blank and then multiplied by the semester (which is 1 for DHYG 125, 2
for DHYG 215, and 3 for DHYG 225). The difficulty level increases with each semester.

Total # of Errors _5_ multiplied by Semester = 3
Adjusted Error total = 15

**Final Score Calculation**

You must now calculate the total General Evaluation Points at the top left of the page. Complete areas that were not
previously evaluated and total the points the student received. Example: the score was 45/50

Calculus Detection Level  23.24 + General Evaluation Points (50) = Total Point Value = 83.24

Add General Evaluation Errors + Adjusted Error Total = 12
5 + 15 = 20

Adjusted Error Total - Total Point Value = 83.24 – 20 = 63.24

Final Points + Total Point Value = 63.24 + 83.24 = 76%
FSU DENTAL HYGIENE PROGRAM
DHYG 233 STUDENT PERFORMANCE FORM

Student: ________________________________________________

Patient Case Type: __________

Periodontal Disease: Chronic-G____ Chonic-L____ Aggressive-G____ Aggressive-L____ Active____ Inactive____ Other____

Medically Compromised: ______ Geriatric (65 & up): __________ Special Needs: __________ Adolescent (12-18): __________

General Evaluation Points: ____________________________ Instr. Initials: __________

Medical History/ASA Class: 5/3/0 ______
Oro Exam/Hard Tissue Chart: 5/3/0 ______
Perio Assessment/Case Type: 10/5/0 ______
Calculus Detection*: 10/5/0 ______
Patient Ed/Care Plan/PT Eval: 5/3/0 ______
Legal Documentation: 5/3/0 ______
Asepsis: 5/3/0 ______
Time Management (use form): 5/3/0 ______

*Calculus Detection Errors: 0=10, 1-3=5, 4-6=0
not an error if the difference is between level 2/3 calculus.

Instructor Feedback: ____________________________________

Time goal after check-in ______ Actual time ______

Total (faculty) ______ ÷ 6 = Avg. ______ x ______

Total number of teeth in dentition ______ = ______

Calculus Level:

1 = Light (L) Calculus – fine, granular, grayish, located along line angles, marginal areas, and/or under contacts. Slight vibration or roughness detected with explorer.

2 = Moderate (M) Calculus – a bump with thickness readily discernible, a marginal ring or interproximal “click” with explorer, definite vibration felt with explorer, a “jump.”

3 = Heavy (H) Calculus – ledge encircling tooth, thick and dense files interproximal space or is a marginal ledge, definite vibration, sometimes “binds” explorer.

Debridement Error Legend:
C = Calculus S = Stain
P = Plaque T = Tissue Trauma

Total # of errors ______ x Semester ______ = ______

Adjusted Error Total:

Semester: DHYG 126 = 1
Semester: DHYG 222 = 2
Semester: DHYG 233 = 3

Instr. Initials: __________

Calculus Level ______ + General Evaluation Points ______ 50 = Total Point Value

Subtract (General Evaluation Errors ______ + Adjusted Error Total ______) = ______

Final Points ______ + Total Point Value = ______%

Comments: ____________________________________________

Medical Alerts: _______________________________________

Recommended Recare Frequency: _________________________

Month ______ Year ______

<table>
<thead>
<tr>
<th>Appointment</th>
<th>One</th>
<th>Two</th>
<th>Three</th>
<th>Four</th>
<th>Five</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finish Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instructor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Student Performance Form Instructions

The student must have a medical history check in with the section instructor before proceeding with the evaluation. To assess points in the General Evaluation Section use the following criteria. The instructor should give the student a time goal in DHYG 225 to help the student become more efficient and to be able to adapt to the office setting. Please refer to the manual form “Student Time Management in Clinic.”

Example

<table>
<thead>
<tr>
<th>Evaluation area</th>
<th>Errors</th>
<th>Points Awarded</th>
<th>Documentation</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical History</td>
<td>None</td>
<td>5</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
<tr>
<td>Medical History</td>
<td>One Error</td>
<td>3</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
<tr>
<td>Medical History</td>
<td>Two Errors or more</td>
<td>0</td>
<td>Circle points received</td>
<td>Instructor initials</td>
</tr>
</tbody>
</table>

Calculus detection will be on designated tooth, if a patient is missing one of the designated teeth, cross off the assigned tooth and insert an adjacent tooth. Example: if #3 is missing select #2. The legend provides the level of calculaus present on the tooth.

To determine the calculaus level, total the numbers assigned for calculaus detection on each of the six teeth evaluated. Once a total number has been added, that total is then divided by 6 (the number of the teeth evaluated for calculaus.) To get a calculaus detection level, multiple the total number of teeth the patient has by the calculaus average.

Calculus Detection (Example)

<table>
<thead>
<tr>
<th>Student</th>
<th>Faculty</th>
<th>Note: The student identifies calculaus level and records in the blanks</th>
</tr>
</thead>
<tbody>
<tr>
<td>#3</td>
<td>2</td>
<td>If the instructor then identifies calculaus level and records in blanks,</td>
</tr>
<tr>
<td>#9</td>
<td>1</td>
<td>whether or not if is the same number as the student’s.</td>
</tr>
<tr>
<td>#14</td>
<td>1</td>
<td>Multiple by number of teeth in dentition = 28</td>
</tr>
<tr>
<td>#19</td>
<td>0</td>
<td>28 x .83 = 23.24</td>
</tr>
<tr>
<td>#30</td>
<td>2</td>
<td>Equals Calculus Level 23.24</td>
</tr>
</tbody>
</table>

Since there are 3 calculaus detection errors, the student would receive 3 points for Calculus Detection under General Evaluation Points. Calculus Detection will be graded as follows: 0-1 error = 10 points, 2-3 errors = 5, and 4-6 errors = 0 points.

Calculus, Plaque, Stain Removal Evaluation

After the student has completed the scaling/unscaling or scaling and polishing a final evaluation is done. Next to each tooth is a blank that will ONLY have items from the legend on it if errors are noted (calculaus, plaque/stain and or tissue trauma is present) after the instructor checks. After the instructor has checked the dentition, an example of how the results could be is as follows: #3 P.C.T, indicating that the instructor found plaque/stain, calculus and tissue trauma on #3, #18 P and #25 C. The total number of errors is 5.

Adjusted Error Total Calculation

To calculate the adjusted error total, the total errors noted under the Final Evaluation section is added together. The total errors is documented in the Total number of errors blank and then multiplied by the semester (which is 1 for DHYG 125, 2 for DHYG 215, and 3 for DHYG 225). The difficulty level increases with each semester.

Total # of Errors _5_ multiplied by Semester = 3
Adjusted Error total = 15

Final Score Calculation

You must now calculate the total General Evaluation Points at the top left of the page. Complete areas that were not previously evaluated and total the points the student received. Example: the score was 45/50

Calculus Detection Level 23.24 + General Evaluation Points (50) = Total Point Value = 83.24

Add General Evaluation Errors + Adjusted Error Total = 12
5 + 15 = 20

Adjusted Error Total - Total Point Value = 83.24 - 20 = 63.24

Final Points + Total Point Value = 63.24 + 83.24 = 76%
DHYG 208 CASE STUDY/JOURNAL INFORMATION REQUEST FORM

NEED THIS FORM FILLED OUT 3 DAYS IN ADVANCE

I understand as a student of Ferris State University Dental Hygiene Clinic, the use and disclosure of patient information is governed by the rules and regulations established under HIPAA and the HITECH Act.

I will use and disclose confidential health information solely in accordance with the federal and university policies set forth. I also understand and agree that my failure to fulfill any of the obligations set forth in the HIPAA confidentiality agreement shall result in my being subject to appropriate disciplinary action up to and including criminal, civil, and university set penalties.

TODAY’S DATE: ________________________

PATIENT NAME __________________________ (PRINT CLEARLY) DOB ________________

_____ PERIO CHART
_____ HARD TISSUE CHART
_____ MEDICAL HISTORY/MEDICATION LIST
_____ SERVICES RENDERED
_____ XRAYS-----DIGITAL OR NORMAL(CIRCLE ONE) DATE______________TYPE- FMX BWX PAN

STUDENT NAME __________________________ DATE NEEDED BY _______________________

YOUR EMAIL ADDRESS ____________________________

Ferris State University
College of Health Professions

DHYG 208 CASE STUDY/JOURNAL INFORMATION REQUEST FORM

NEED THIS FORM FILLED OUT 3 DAYS IN ADVANCE

I understand as a student of Ferris State University Dental Hygiene Clinic, the use and disclosure of patient information is governed by the rules and regulations established under HIPAA and the HITECH Act.

I will use and disclose confidential health information solely in accordance with the federal and university policies set forth. I also understand and agree that my failure to fulfill any of the obligations set forth in the HIPAA confidentiality agreement shall result in my being subject to appropriate disciplinary action up to and including criminal, civil, and university set penalties.

TODAY’S DATE: ________________________

PATIENT NAME __________________________ (PRINT CLEARLY) DOB ________________

_____ PERIO CHART
_____ HARD TISSUE CHART
_____ MEDICAL HISTORY/MEDICATION LIST
_____ SERVICES RENDERED
_____ XRAYS-----DIGITAL OR NORMAL(CIRCLE ONE) DATE______________TYPE- FMX BWX PAN

STUDENT NAME __________________________ DATE NEEDED BY _______________________

YOUR EMAIL ADDRESS ____________________________