HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

DENTAL HYGIENE

POLICIES AND PROCEDURES

2024

Table of Contents

Ferris State University Dental Hygiene Clinic is defined as a health provider and a covered entity by HIPAA. We conduct certain financial, administrative, as well as dental radiographic (dental identifiable radiographs) transactions electronically and possess individually identifiable health information. We will comply with all the requirements of the HIPAA Privacy Rule 2013.

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-healthcare 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.

I. Important definitions and Concepts Used in These Policies and Procedures

These Policies and Procedures use several important terms and concepts in describing the FSU Dental Hygiene Clinic obligations under the Privacy Rules. All definitions in the Privacy Rules are hereby incorporated by reference into these Policies and Procedures. If a term is not defined in the Privacy Rules, the term shall have its generally accepted meaning. Several of the key terms and concepts from the Privacy Rules are:

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.

CFR: The Code of Federal Regulations- codification of the general and permanent rules and regulations published in the Federal Register by executive departments and agencies of the federal government of the United States which is updated periodically.

Covered Entity: Covered Entity Under HIPAA includes a health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Standards for Electronic Transactions (45 CFR 162.100 et seq.)

De-identified Information: Protected health information under HIPAA is *individually identifiable* health information. De-*Identifiable* data is data that has been stripped of all data that is explicitly linked to a particular individual (that's *identified* information) and health information with data items which reasonably could be expected to allow individual identification. See also 45 CFR 160.103, 45 CFR 164.502(d)

Designated Record Set: The Designated Record Set is defined as records (paper or electronic) maintained by the Dental Hygiene Clinic that are of dental and billing records about patients; or the enrollment, payment, claims adjudication, and case or electronic management record systems; and/or used, in whole or in part, by the Dental Hygiene Clinic to make decisions about patients.

Disclosure: Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. [45 CFR 160.103]

Health Care Operations: Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1. conducting quality assessment and improvement activities, population-based activities, and related functions that do not include treatment
2. reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and health plan performance, conducting training programs where students learn to practice or improve their skills as health-care providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities

3. underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits;
4. conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. business management and general administrative activities of the entity. [45 CFR 164.501]

Limited Data Set: Protected Health Information that excludes the following identifiers of the individual, or of relatives, employers or household members of the individual: names, postal address information other than town or city, state and zip code, telephone numbers, fax numbers, electronic mail address, social security number, health plan beneficiary number, account number, certificate/license number, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), Internet Protocol (IP) address numbers, biometric identifiers, including finger and voice prints and full face photographic images and any comparable images.

Minimum Necessary: One of the guiding principles behind the HIPAA Privacy Rule is the "minimum necessary standard." This standard requires a health care provider to limit the use, disclosure of and requests for protected health information to the minimum necessary to accomplish legitimate tasks. [45 CFR 164.514(d)(1)]

Payment: 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.

Protected Health Information (PHI): Health Information about an individual that is electronically transmitted or stored information; Created or received by a health care provider—written or oral; Related to the past, present or future physical or mental condition of an individual, or the provision of health care for an individual; that Includes demographic information, which can be used to identify the individual. PHI includes demographic information, dates of service, diagnosis, nature of services, medical treatment department and other information that may reveal the identity of the individual or any facts about his or her health care or health insurance. HIPAA allows only demographic patient information, health insurance status, dates of service, department of service information, treating physician information and (for limited purposes) outcome information to be used for fundraising purposes without written patient authorization.

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information with an entity that maintains such information. [45 CFR 160.103.]

Information about an individual is no longer considered PHI once the individual has been deceased more than 50 years. Therefore, the Dental Hygiene Clinic is not obligated to apply these policies and procedures to health information about an individual who has been deceased for more than 50 years.

Workforce member: Under HIPAA, this means employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity. Also see Part II, 45 CFR 160.103.

II. Health Plan's Responsibilities as a Covered Entity

A. Privacy Officer and Contact Person

The Privacy Rules require the FSU Dental Hygiene Clinic to appoint a privacy official ("Privacy Officer") who is responsible for developing and implementing privacy policies and procedures. The Privacy Rules also require the FSU Dental Hygiene Clinic to appoint a contact person or office who is responsible for receiving complaints of privacy violations and who can provide more information about the Notice of Privacy Practices that the FSU Dental Hygiene Clinic is required to send all participants in the Dental Hygiene Clinic. the FSU Dental Hygiene Clinic has established the following administrative structure designed to comply with these requirements:

- The Privacy Officer, who has overall responsibility for the privacy and security of PHI. The Privacy Officer is the Dental Hygiene Clinic Operations Supervisor and can be contacted at 231-591-2284.

B. Workforce Training

The FSU Dental Hygiene Clinic policy is that all members of its workforce involved in the administration of its Dental Hygiene Clinic or who otherwise need access to PHI will be trained as necessary and appropriate for them to carry out their functions. For purposes of these Policies and Procedures, the FSU Dental Hygiene Clinic workforce includes employees, dental hygiene students, volunteers, trainees, interns/externs, workers employed by a temporary agency, independent contractors, and any other persons whose work performance is under the direct control of the FSU Dental Hygiene Clinic's, whether they are or not paid by FSU.

The Privacy Officer is responsible for developing training schedules and programs so that all appropriate workforce members receive the training necessary and appropriate for them to carry out their functions for the Dental Hygiene Clinic. Newly hired employees and dental hygiene students will be trained before they are given access to PHI, or as soon as possible thereafter. All training will be documented as set forth in the Privacy Rules' documentation requirements. (See section III. M, "Documentation and Record Retention Requirements").

C. Safeguards

The FSU Dental Hygiene Clinic has in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. The "HIPPA Security Rule Safeguards for the Dental Hygiene Clinic" is maintained to provide the details of confidential

Administrative, Physical and Technical Safeguards for the protection of ePHI.

Administrative safeguards. The FSU Dental Hygiene Clinic Policies and Procedures include a number of administrative safeguards to protect the privacy of PHI. These administrative safeguards include:

- Appointment of the Privacy Officer to implement and oversee compliance with the Policies and Procedures
- Training of workforce members regarding the Policies and Procedures at least annually
- Risk Assessment and Management
- Creation of administrative firewalls between the FSU Dental Hygiene Clinic functions and its employment or educational functions

Technical safeguards. The FSU Dental Hygiene Clinic has adopted the following technical safeguards to protect the privacy of PHI on its computer systems, use of telephones, mail, fax machines, and email:

- Restriction of access to PHI on its computers to individuals who need access to PHI to perform their duties.
- Use of passwords to authenticate an individual's right to access PHI.
- Creation of computer firewalls around PHI to protect it from unauthorized access by others within or outside the FSU Dental Hygiene Clinic.
- Changing of computer passwords on a routine basis.
- Workforce members "locking" the computer when they leave it unattended.
- Sending encrypted electronic mail when communicating with dental patients or dental offices whenever feasible.
- Confirmation calls may be made by telephones in VFS 205 or the Dental Hygiene Clinic office
    - messages and appointment reminders may be left on answering machines and voicemail systems but LIMIT the amount of information disclosed in a telephone message
- Workforce members shall not use cell phones and other personal devices that can record sound or images around PHI unless it is related to a business application.
    - Cell phones and their cameras are prohibited in the clinical areas, unless needed for business related purposes. Example: cell phone is needed for work functions by ITSC, DH Privacy Officer or other authorized users. Special permission may be granted to use in the event of emergencies. A Standard Operating Procedure (SOP) has

been developed that all faculty/staff/ students are made aware of via memo or through orientation and Castlebranch.

- Faxes: Fax machines MUST be in secure areas that cannot be easily accessed by visitors or patients.

Physical safeguards. The FSU Dental Hygiene Clinic has adopted the following physical safeguards to protect the privacy of PHI

- Paper files containing PHI are kept in locked filing cabinets and must not leave the FSU Dental Hygiene Clinic area
    - i.e. dental charts, student grade sheets and recall logs
- Only workforce members with responsibility for the dental clinic have access to dental records.
- Door Scan cards are used by workforce members with access to areas containing PHI and the dental clinic.
    - Restricted times are enforced for some workforce members
    - Reports are created to monitor workforce members entering areas containing PHI.
- Electronic dental information is accessed by workforce members who need access to such information. This includes electronic health information maintained internally (i.e. FSU information systems) and externally (i.e., third party administer websites).
- Electronic records in Ascend Academic are accessible only on university computers in the VFS building.
- The clinic operations supervisor, dental clinic clerk, and program coordinator are the only staff with access off site.
- Reasonable precautions are taken to ensure that paper files are not left out in the open or unattended.
- Any equipment that potentially has PHI stored on it is destroyed appropriately to protect the privacy of information.
- Shredder boxes are in VFS 201, 202 and 204 for proper disposal of documents containing PHI.
- Mail: Send mail to the patient's primary address unless the patient requests an alternative address. Postcards may be used for appointment reminders and the postcard contains the MINIMUM NECESSARY amount of patient information.
- Avoid discussing PHI where others can hear and lower voice when speaking in the presence of other patients.

D. Complaints

The Privacy Rules require the FSU Dental Hygiene Clinic to implement a process by which individuals may file complaints about privacy violations. The FSU Dental Hygiene policy is that anyone who believes that the Policies and Procedures or the Privacy Rules have been

violated at the FSU Dental Hygiene may submit a written complaint to the Privacy Officer.

Any individual who wishes to file a complaint should request from the Privacy Officer the *Individual Complaint form*. Upon receiving a completed complaint form, the Privacy Officer will do the following:

- Review the Policies and Procedures or Privacy Rules at issue
- Obtain any additional information from the individual necessary to understand the nature and basis of the complaint
- Investigate the conduct that is the subject of the complaint, which may include interviewing members of the workforce and business associates, and reviewing records in the individual's designated record set
- If appropriate, consult with legal counsel or other appropriate resources for evaluating the complaint
- Decide how the complaint will be handled and then take appropriate action, which may include:
    - Actions necessary to minimize any harmful effects from the unauthorized use or disclosure
    - Disciplinary action again workforce members in accordance with the FSU Dental Hygiene Clinic disciplinary policies (see section II. E, "Discipline")
    - Appropriate sections with respect to business associates in accordance with the relevant business associate agreement (see section III. I, "Uses and Disclosures of PHI by Business Associates")
    - Modification of the Policies and Procedures, if necessary
    - No action, if it is determined that there has been no violation of the Policies and Procedures or the Privacy Rules
- Communicate to the individual, in writing and on a timely basis, the final outcome of the complaint investigation.
- Retain documentation of the complaint and its disposition as required by the Privacy Rules' document requirements (see section III. M, "Documentation and Record Retention Requirements")
- Complete the *Complaint Tracking Form*

E. Discipline

The Privacy Rules require the FSU Dental Hygiene Clinic to have and apply appropriate discipline to workforce members who fail to comply with the Policies and Procedures or the Privacy Rules. The FSU Dental Hygiene Clinic policy is to appropriately discipline any employee who violates the Policies and Procedures or the Privacy Rules.

Type of Discipline. The FSU Dental Hygiene Clinic will appropriately discipline workforce members who fail to comply with the Policies and Procedures or the Privacy Rules, in accordance with the disciplinary policies set forth in each workforce member specific handbook, The FSU Dental Hygiene 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 the FSU Dental Hygiene will not discipline employees who disclose PHI, as long as:

- the employee believes in good faith that the FSU Dental Hygiene Clinic has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Dental Hygiene Clinic potentially endangers one or more patients, workers, or the public;
- disclosure of PHI is necessary to revealing the conduct, and the disclosure is no more than reasonably necessary to establish the unlawful or unprofessional conduct; 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. The FSU Dental Hygiene Clinic 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).

F. No Intimidating or Retaliatory Acts

The FSU Dental Hygiene Clinic will not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.

G. No Waiver of Rights

The FSU Dental Hygiene Clinic will not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment and enrollment or other benefits eligibility.

H. Notice of Privacy Practices

The Privacy Rules require the FSU Dental Hygiene Clinic to provide participants in the Dental Hygiene Clinic with a notice describing (1) how the Dental Hygiene may use and disclose their PHI; (2) individuals' rights under the Privacy Rules; and (3) the Dental Hygiene Clinic's legal duties with respect to PHI. the FSU Dental Hygiene policy is to create and distribute such a notice ("Notice of Privacy Practices" or "Notice") as required by the Privacy Rules.

Creating the Notice. The Privacy Officer is responsible for developing and maintaining the FSU Dental Hygiene Clinic's Notice. The Privacy Officer also must ensure that the Notice complies with the requirements set forth in the Privacy Rules and that a copy of the Notice is maintained in accordance with the "Documentation and Retention Requirements (see section III. M, "Documentation and Record Retention Requirements").

Contents of the Notice. The Notice of Privacy Practices shall describe:

- the uses and disclosures of PHI that may be made by the Dental Hygiene Clinic
- the individual's rights
- the Dental Hygiene Clinic's legal duties with respect to PHI

Delivering the Notice. The Privacy Officer will ensure that that Notice is delivered to participants in the Dental Hygiene Clinic as follows:

- A hard copy will be available to each new patient in the Dental Hygiene Clinic
- The Notice of Privacy Practices will be posted on the web site and electronically available.
- If a change or revision to the Notice of Privacy Practices occurs, it will be updated on the FSU website.

At least once every three years, the FSU Dental Hygiene Clinic will inform all patients that the Notice is available and how they can obtain a copy. The FSU Dental Hygiene Clinic will also provide a copy of the Notice to any individual upon request.

III. Procedures for Uses and Disclosures of PHI

A. Who Must Comply with These Policies and Procedures

All the FSU Dental Hygiene Clinic workforce members must comply with the Policies and Procedures.

B. Limitations on Access to PHI

The FSU Dental Hygiene Clinic limits access to PHI to employees with certain job functions ("Authorized Employees"). These Authorized Employees either perform functions directly on behalf of the Dental Hygiene Clinic, or they access PHI on behalf of the FSU Dental Hygiene Clinic for its use in administering the dental hygiene care. Authorized Employees are:

- Privacy Officer
- Associate Dean of College of Health Professions (CHP)
- Others authorized or designated by the Associate Dean CHP & Privacy Officer
- Dental hygiene and work study students
- Dental clinical clerks
- Dentists, faculty, staff, and dental hygiene students who provide dental care.
- The FSU IT department

These Authorized Employees may use and disclose PHI to perform or support dental care functions, and they may disclose PHI to other Authorized Employees who perform or support dental hygiene care functions. Such uses and disclosures, however, must be limited to the minimum necessary to perform or support dental hygiene care functions. Routine uses and disclosures must be made in accordance with departmental procedures (see section V.E., "Departmental Minimum Necessary Policies and Procedures"). Non-routine uses and disclosures must be approved by the Privacy Officer. Authorized Employees may not disclose PHI to employees not identified in this section, except in accordance with these Policies and Procedures.

C. Permitted Uses and Disclosures

The FSU Dental Hygiene Clinic is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

a. To the Individual (unless required for access or accounting of disclosures);
b. Treatment, Payment, and Health Care Operations;
c. Opportunity to Agree or Object;
d. Incident to an otherwise permitted use and disclosure;
e. Public Interest and Benefit Activities; and
f. Limited Data Set for the purposes of research, public health or health care operations. The Dental Clinic may rely on

professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Questions about Uses and Disclosures for Payment and Health Care Operations. Any FSU Dental Hygiene Clinic employee who is unsure as to whether a particular task that involves use or disclosure of PHI qualifies as a payment activity or health care operation of the Dental Hygiene Clinic must contact the Privacy Officer.

D. Mandatory Disclosures of PHI to Individuals and HHS

The Privacy Rules require the FSU Dental Hygiene Clinic to disclose an individual's PHI when requested by the individual or, under certain circumstances, by the Department of Health and Human Services. the FSU Dental Hygiene Clinic policy is to cooperate with these requests and to disclose the PHI in accordance with the Privacy Rules.

Requests from the Individual. An individual (or the individual's personal representative) may request a disclosure of his or her own PHI. The FSU Dental Hygiene Clinic will respond to such requests by following the procedures under "Individual's Request to Inspect and Copy" (see section IV. A).

Request from the Department of Health and Human Services (HHS). The FSU Dental Hygiene Clinic will respond to a request from an HHS official for disclosure of PHI as follows:

- verify the identity of the HHS official using the procedures set forth in the section entitled "Verifying the Identity of Those Requesting PHI" (see section III. L)
- document the disclosure as required under the Privacy Rules' documentation requirements (see section III. M, "Documentation Requirements")

E. Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes

From time to time, the FSU Dental Hygiene Clinic may receive requests from courts, parties to litigation, law enforcement officials, public health authorities, or various other government agencies or officials to use or disclose an individual's PHI. The Privacy Rules set forth guidelines under which the FSU Dental Hygiene Clinic may use or disclose PHI in such circumstances. The FSU Dental Hygiene Clinic policy is that the FSU Dental Hygiene Clinic may respond to such a request only if the use or disclosure meets the following conditions:

- The FSU Dental Hygiene Clinic Privacy Officer approves the use or disclosure after consultation with legal counsel
- the disclosure complies with the minimum necessary standard or is specifically exempted from the minimum necessary standard (see section V, "Procedures for Complying with the Minimum Necessary Standard")
- the disclosure falls within one of the following categories, and the specific requirements set forth in the Privacy Rules have been followed (see section 164.512 of the Privacy Rules):
    - in response to an order of a court or an administrative tribunal
    - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, provided that there is an appropriate protective order in place and, where medical records are involved, the individual has waived his or her physician-patient privilege
    - pursuant to process (such as a court-ordered warrant or an administrative summons) and as otherwise required by law
    - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual 16 who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on the FSU Dental Hygiene Clinic premises
    - about an individual that the FSU Dental Hygiene Clinic reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information
    - to appropriate public health authorities for public health activities
    - to a health oversight agency for health oversight activities
    - to coroners, medical examiners, and funeral directors about a deceased individual
    - for cadaveric organ, eye or tissue donation purposes
    - for certain research purposes, when the need for an authorization has been waived or is otherwise not required
    - in order to avert a serious threat to health or safety
    - about armed forces personnel to appropriate military command authorities

    - for national security and intelligence activities
    - for protective services to the President of the United States and other designated persons
    - to correctional institutions and law enforcement custodians
    - in connection with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault
- if the disclosure is to a public official, verify the identity of the public official using the procedures set forth in "Verifying the Identity of Those Requesting Potential Health Information" (see section III.L)
- the disclosure complies with any additional restrictions under state laws for the right to use or disclose PHI
    - in a Michigan court case, medical records are subject to a privilege. If the FSU Dental Hygiene Clinic receives a subpoena, the FSU Dental Hygiene Clinic may not release a party's medical records without an accompanying court order, administrative order, or patient's waiver of the physician-patient privilege (see Mich. Ct. Rule 2.314)
- document the disclosure according to the Privacy Rules' documentation requirements (see section III. M, "Documentation and Record Retention Requirements"), except that documentation is not required if the disclosure is for:
    - national security or intelligence purposes; or
    - to correctional institutions or law enforcement custodians

F. Use of PHI for Marketing

The FSU Dental Hygiene Clinic's general policy is not to use PHI for marketing activities. Any use of PHI for marketing would require approval by the Privacy Officer. Before any such marketing use could occur, the FSU Dental Hygiene Clinic would first have to obtain authorization from each individual whose information was to be used for marketing purposes (see III. H, Uses and Disclosures of PHI with an Individual's Authorization).

Definition. "Marketing" is any communication about a product or service that encourages the recipients to purchase the product or service. However, the following communications require no authorization even though the actions may constitute marketing:

- Face to face communication (not including conversations over the phone).
- Promotional gifts of nominal value.
- Communications promoting health in general and that do not promote a product or service from a particular provider, such as communications promoting a healthy diet or encouraging individuals to receive certain routine diagnostic tests.
- Communications about government and government-sponsored programs such as communications regarding Medicare or Medicaid eligibility.

Marketing also does not include communications made for the following purposes, unless the FSU Dental Hygiene Clinic is paid by a third party to do make the communication:

- Treatment.
- Case management/care coordination or recommending alternative treatments.
- To describe a dental-related product or service provided by the covered entity including participation in a dental care provider network or dental plan network; replacement of or enhancements to a dental plan; dental related products or services available only to a dental plan enrollee that add value to but are not part of a plan of benefits.

G. Sale of PHI

The FSU Dental Hygiene Clinic's general policy is not to sell PHI of those covered under the Dental Hygiene Clinic. Any sale of PHI would require approval by the Privacy Officer. Before such a sale could occur, the FSU Dental Hygiene Clinic would first have to obtain authorization from each individual whose information was to be sold (see III.H, Uses and Disclosures of PHI with an Individual's Authorization).

Definition. "Sale of PHI" means any disclosure of PHI where the FSU Dental Hygiene Clinic receives direct or indirect remuneration from the recipient of the PHI.

Exceptions. There are several exceptions to what constitutes a sale of PHI under HIPAA. A sale does not include the following, and the FSU Dental Hygiene Clinic will not seek an individual's authorization for the following disclosures:

- For public health activities described in 45 CFR § 164.512(b) or § 164.514(e).

- For research, where the only remuneration received by the FSU Dental Hygiene Clinic is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for those purposes.
- For treatment and payment.
- For the transfer, merger, or consolidation of all or part of the FSU Dental Hygiene Clinic and related due diligence.
- To a business associate for activities that the business associate undertakes on behalf of the FSU Dental Hygiene Clinic if the only remuneration is provided by the FSU Dental Hygiene Clinic to the business associate for its performance of such activities.
- Providing an individual with access to his or her PHI.
- For disclosures required by law.
- For any other purposes permitted by and in accordance with the applicable requirements of the Privacy Rule, where the only remuneration received by the FSU Dental Hygiene Clinic is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose, or a fee that is otherwise expressly permitted by other law.

H. Uses and Disclosures of PHI with an Individual's Authorization

The Privacy Rules provide that unless expressly authorized by the individual who is the subject of the PHI (or the individual's personal representative), any use or disclosure of that individual's PHI is prohibited unless it falls within one of the categories for which disclosure is permitted or required or the individual has been deceased for at least fifty years. An individual may, however, expressly authorize a use or disclosure of PHI for any purpose.

The FSU Dental Hygiene Clinic's policy is that any use or disclosure made pursuant to an authorization may be made only if the FSU Dental Hygiene Clinic: (1) determines that the authorization is valid (as described below); (2) verifies the identity of the individual who signed the authorization (see section III. L, "Verifying the Identity of Those Requesting PHI"); and (3) ensures that the use or disclosure is made consistent with the terms of the authorization.
Valid Authorizations. An authorization is valid only if it is written in plain language and contains the following required core elements and statements:

Core Elements. In order to be valid, an authorization must contain all of the following core elements:

- a specific and meaningful description of the PHI to be used or disclosed
- the name or other specific identification of the person or class of persons authorized to use or disclose the PHI
- the name or a description of the person or class of persons to whom the FSU Dental Hygiene Clinic may make the requested use or disclosure
- the purpose(s) of the requested use or disclosure. (If the individual initiates the authorization and does not provide a statement of purpose, the statement "at the request of the individual" is sufficient)
- a valid expiration date (e.g., Month, Day, Year) or expiration event (e.g., termination from a dental plan, rejection of an insurance application, etc.)
- the signature of the individual and the date the authorization was signed. (If signed by the individual's personal representative, a description of the representative's authority to act for the individual must also be provided)

Required Statements. In order to be valid, an authorization must contain all of the following statements:

- a statement of the individual's right to revoke the authorization in writing, and either (1) a list of the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (2) a reference to the Notice of Privacy Practices, if the Notice lists the exceptions to the right to revoke and provides a description of how the individual may revoke the authorization
- a statement informing the individual that:
  The FSU Dental Hygiene Clinic may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization; or the consequences to the individual if he or she refuses to sign the authorization when:
    - the authorization is to be used to for the Dental Plan's eligibility or enrollment determinations or for its underwriting or risk rating determinations; or
    - a covered entity will be providing dental hygiene care solely for the purpose of creating PHI for disclosure to a third party and the authorization is to allow the disclosure to the third party (e.g., a physician releasing the results of medical conditions to the FSU Dental Hygiene Clinic)

Providing a Copy of the Authorization to the Individual. If the FSU Dental Hygiene Clinic is seeking the authorization from the individual, the FSU Dental Hygiene Clinic must provide the individual with a copy of the signed authorization.

Revoking an Authorization. An individual may revoke an authorization at any time, although the revocation will not be effective to the extent that the FSU Dental Hygiene Clinic has already used or disclosed information in reliance on the authorization.

Documentation Required. A copy of the authorization must be maintained as required under the Privacy Rules' documentation requirements (see section III.M, "Documentation and Record Retention Requirements").

I. Uses and Disclosures of PHI by Business Associates Business Associate Agreements.

Business Associate Agreements. The Privacy Rules require that before the FSU Dental Hygiene Clinic may share PHI from the Dental Plan with outside service providers, the outside service providers must contractually obligate themselves to protect the PHI. The FSU Dental Hygiene Clinic's policy is that it will not share PHI with a third party that performs services for the Dental Hygiene Clinic until that party has entered into an agreement in which the party agrees to appropriately protect PHI.

The Privacy Rules call these third parties that provide services to or on behalf of the Dental Hygiene Clinic "business associates." A copy of the business associate agreement must be maintained according to the Privacy Rules' documentation requirements (see section III. M, "Documentation and Record Retention Requirements").

Uses and Disclosures of PHI by Business Associates. The FSU Dental Hygiene Clinic may provide PHI to a business associate under the following conditions:

- the FSU Dental Hygiene Clinic has verified that a valid business associate contract is in place
- the disclosure is consistent with the terms of the business associate agreement
    - the disclosure complies with the minimum necessary standard (see section V, "Procedures for Complying with the Minimum Necessary Standard")

- the disclosure is documented in accordance with the Privacy Rules' documentation requirements (see section III.M, "Documentation and Record Retention Requirements"), unless such documentation is unnecessary because the disclosure falls within one of the following categories:
    - payment or health care operations
    - mandatory disclosures of PHI to an individual or to HHS
    - national security and intelligence activities
    - correctional institutions and law enforcement custodians under a valid authorization that is retained as required by the Privacy Rules' documentation requirements (see section III. M, "Documentation Requirements")

Unauthorized Uses and Disclosures of PHI by Business Associates. If the FSU Dental Hygiene Clinic learns that a business associate has used or disclosed PHI in an unauthorized manner, the FSU Dental Hygiene Clinic will take the following steps:

- the Privacy Officer will immediately notify the business associate in writing of the alleged unauthorized use or disclosure
    - the Privacy Officer will telephone the business associate to discuss the alleged unauthorized use or disclosure and to determine whether the unauthorized use or disclosure will cease
- if the business associate does not agree to stop the unauthorized use or disclosure, if the FSU Dental Hygiene Clinic learns that the use or disclosure has not stopped, or if the unauthorized use or disclosure is part of a pattern of conduct in violation of the business associate's agreement with the FSU Dental Hygiene Clinic, then the FSU Dental Hygiene Clinic will:
    - terminate its relationship with the business associate; or
    - if termination is not possible (for example, because there is no other entity in the area that can provide the service), then the FSU Dental Hygiene Clinic will report the business associate to the Department of Health and Human Services
- the Privacy Officer will document the known details of the unauthorized use or disclosure for purposes of responding to requests for an accounting of disclosures (see section IV. C)
- if appropriate, the Privacy Officer will follow the procedures set forth in "Mitigation of Inadvertent Disclosures of PHI" (see section III. N)

- the Privacy Officer will follow the Breach Notification Policy contained (see section III.N)

J. Requests for Disclosure of PHI from Spouses, Family Members, and Friends

From time to time, the FSU Dental Hygiene Clinic may receive requests from spouses, family members, or friends of an individual seeking that individual's PHI. The Privacy Rules allow such disclosures only under very limited circumstances. Normally, an individual's PHI may be released to a spouse, family member or friend only if the individual has signed an authorization allowing such disclosure or in emergency situations if the Privacy Officer concludes that the disclosure is in the individual's best interest. The FSU Dental Hygiene Clinic's policy is to release an individual's PHI to a spouse, family member, or friend only as allowed under the Privacy Rules.

The FSU Dental Hygiene Clinic may disclose PHI of an individual to a spouse, family member or friend of the individual only under the following circumstances:

- the individual whose PHI is involved has provided a valid authorization allowing disclosure to the spouse, family member or friend, in which case the procedures under the section "Uses and Disclosures of PHI with an Individual's Authorization" must be met (see section III. H)
- the family member is (1) the parent of the individual whose PHI is involved and (2) the individual is a minor child, in which case the procedures under the section "Verifying the Identity of Those Requesting PHI" must be met (see section III. L); or
- the spouse, family member or friend is the personal representative of the individual whose PHI is involved, in which case the procedures under the section "Verifying the Identity of Those Requesting PHI" must be met (see section III. L)

Information about Deceased Individuals. If the FSU Dental Hygiene Clinic receives a request for information from a family member, other relative, or a close personal friend of the individual who were involved in the individual's care or payment for health care prior to the individual's death, the FSU Dental Hygiene Clinic, at its discretion, may disclose the information relevant to that person's involvement, unless doing so is inconsistent with any prior

expressed preference of the individual that is known to the FSU Dental Hygiene Clinic.

Emergency Disclosure of Information. If the FSU Dental Hygiene Clinic receives a request for information from a person who has not been identified in an authorization form to receive an individual's PHI (and is not otherwise authorized to receive the PHI for purposes of administering the dental hygiene care, the FSU Dental Hygiene Clinic will normally deny the request. In an emergency situation, the Privacy Officer may permit disclosure to a family member or close friend who is involved in the individual's care or payment for the individual's care, if (1) the individual is aware that such disclosure may be made, has had an opportunity to object to the disclosure and does not object; or (2) the FSU Dental Hygiene Clinic is unable to notify the individual about the proposed disclosure and the Privacy Officer determines that the disclosure is in the individual's best interest. Information released in such instances will normally be limited to dental coverage and insurer contact information.

K. Uses and Disclosures of De-Identified Information

Under the Privacy Rules, health information from which all individual identifiers have been removed is called de-identified information and can be used and disclosed without an individual's authorization. The FSU Dental Hygiene Clinic's policy is that information must be approved by the Privacy Officer as de-identified information before it can be disclosed as such.

The FSU Dental Hygiene Clinic may use and disclose de-identified information only if the Privacy Officer has verified that the information is in fact de-identified. De-identified information is not PHI, so once the information has been approved as de-identified information, the FSU Dental Hygiene Clinic may freely use and disclose the de-identified information.

L. Verifying the Identity of Those Requesting PHI.

The Privacy Rules require that the FSU Dental Hygiene Clinic verify the identity and authority of persons or entities exercising their individual rights or otherwise seeking access to PHI. The FSU Dental Hygiene Clinic's policy is to verify both the identity of such person or entity and the authority of the person or entity making the request (if the identity or authority is not known).

Request by the Individual Who Is the Subject of the PHI. The FSU Dental Hygiene Clinic may disclose PHI in response to a request by the individual who is the subject of the PHI by using the following verification procedures:

- *In Person*. If the individual makes the request in person:
  - request and make a copy of a form of identification from the individual, which may consist of a valid the FSU Student/Employee I.D. card, a valid driver's license, a valid passport, or other valid photo identification issued by a government agency
  - verify that the identification matches the identity of the person requesting access to the PHI. If there is any doubt as to the validity or authenticity of the identification, the Privacy Officer must be consulted
  - complete the appropriate sections of the FSU Dental Hygiene Clinic's *HIPAA Verification Check List*, including the signature of the person making the inquiry and the date of the inquiry
  - file the *HIPAA Verification Check List*, along with a copy of the identification, in the designated record set of the individual whose records are being accessed in accordance with the Privacy Rules' documentation requirements (see section III. M, "Documentation and Record Retention Requirements")
  - follow the applicable procedures set forth in "Procedures for Complying with Individual Rights" (see section IV)

- *By Telephone.* If the individual requests PHI over the telephone, inform the individual that it is the FSU Dental Hygiene Clinic's policy not to provide PHI over the telephone. The individual should be instructed to make the request in person, or should be directed to send the request in writing using the appropriate form specified in the applicable "Procedures for Complying with Individual Rights" (see section IV)

- *By E-mail*. If the individual requests PHI through an e-mail request, the receiver is to inform the individual that it is the FSU Dental Hygiene Clinic's policy not to provide PHI in response to an e-mail request. The individual should be instructed to make the request in person, or should be directed to send the request in writing using the appropriate

form specified in the applicable "Procedures for Complying with Individual Rights" (see section IV)

- *In Writing on the Appropriate Form*. If the individual submits a written request for PHI using the appropriate form:
    - ensure that the form has been completely filled out
    - compare the information in the written request with information in the individual's records. If the information does not match, or if there is any doubt as to the identity of the person making the request, contact the Privacy Officer
    - file a copy of the request with the designated record set of the individual whose records are being accessed, in accordance with the documentation requirements (see section III.M, "Documentation and Record Retention Requirements")
    - follow the procedures set forth in "Individual's Request to Inspect and Copy" (see section IV. A)

- *In Writing, But Not on the Appropriate Form*. If the individual submits a written request for PHI without using the appropriate form, disclosure may occur only at the discretion of the Privacy Officer. Absent unusual circumstances, request that the individual fill out the correct form

Request by a Parent of a Minor Child. The FSU Dental Hygiene Clinic may respond to the request made by a parent seeking PHI of the parent's minor child using the following verification procedures:

- verify the identity of the person making the request following the procedures above for responding to a request by an individual
- verify the person's relationship with the child. The relationship may be verified by confirming enrollment of the child as a dependent in the Dental Plan
    - generally, a non-custodial parent shall not be denied access to records or information concerning his or her minor child, unless prohibited by court order
    - verify from the dental records that the child is a minor
- verify from the dental records that there is no restriction in place, such as a court order prohibiting release of information to the parent • follow the appropriate procedures set forth in "Procedures for Complying with Individual Rights" (see section IV)

Request subject to an Authorization. If a person seeks to access an individual's PHI pursuant to an authorization, the FSU Dental Hygiene Clinic will (1) verify the validity of the signature on the authorization form by comparing the signature with a signature in the individual's dental record or other records available to the FSU Dental Hygiene Clinic, and (2) compare other personal information in the authorization form with information in the dental record. The FSU Dental Hygiene Clinic will also take reasonable steps to ensure that the person seeking the records is identified in the authorization. If there is any question as to the validity of the authorization or of the request for information, the FSU Dental Hygiene Clinic may contact the individual who the subject of the PHI is to discuss the validity and scope of the authorization.

Request by a Personal Representative. The FSU Dental Hygiene Clinic may respond to a request for an individual's PHI made by a personal representative of the individual using the following verification procedures:

- verify the identity of the person making the request using the procedures above for responding to a request by an individual
- verify the personal representative's authority to access the individual's record
    - check the individual's file for a copy of a valid power of attorney, order of court, guardianship order, or similar documentation establishing the personal representative's authority. If there is a question as to the scope of authority conferred upon the individual, contact the Privacy Officer to review the document. Advice from legal counsel may also be necessary
    - if the file does not have such documentation
        - obtain a copy of a valid power of attorney, order of court, guardianship order or similar documentation establishing the authority of the personal representative. If there is a question about the validity or sufficiency of the document, or the scope of authority conferred upon the personal representative, contact the Privacy Officer to review the document. Advice from legal counsel may also be necessary.
        - an individual does not have the authority to obtain PHI of his or her spouse without a properly executed authorization from the spouse

        - file a copy of the document in the individual's designated record set according to the documentation requirements (see section III. M)

- follow the appropriate procedures set forth in "Procedures for Complying with Individual Rights" (see section IV)

Request by a Public Official. The FSU Dental Hygiene Clinic may respond to a request for an individual's PHI made by a public official using the following verification procedures:

- verify that the request is for one of the purposes set forth above in the sections entitled "Mandatory Disclosures of PHI to Individuals and HHS" (see section III. D) or "Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes" (see section III. E)
- verify that the person is a public official or acting on behalf of a government agency:
    - if the request is made in person:
        - ask to see an agency identification badge, official credentials, or other proof of government status
        - make a copy of the identification provided, write on it the date of the request, and file it with the individual's designated record set
    - if the request is in writing:
        - verify that the request is on appropriate letterhead
        - make a copy of the writing and file it with the individual's designated record set
    - if the request is by a person purporting to act on behalf of a public official:
        - establish that the individual is acting on behalf of the public official, which may be established by one of the following documents:
        - a written statement on appropriate government letterhead that the person is acting under the government's authority
        - a contract for services with the government agency
        - a memorandum of understanding with the government agency
        - a purchase order with the government agency
        - make a copy of the document and file it with the individual's designated record set

- if there is any question as to the person's identity or affiliation with the government agency, contact the Privacy Officer

- verify that the person is authorized to access the PHI:
  - request a written statement setting forth the legal authority under which the information is being requested
    - if under the circumstances a written statement would be impracticable, obtain an oral statement of such legal authority (and document the oral statement)
    - if the request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact legal counsel
    - make a copy of the document setting forth the legal authority and file if with the individual's designated record set
  - follow the applicable procedures set forth above in the sections entitled "Mandatory Disclosures of PHI to Individuals and HHS" (see section III. D) or "Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes" (see section III. E)

M. Documentation and Record Retention Requirements

The Privacy Rules require the FSU Dental Hygiene Clinic to maintain documentation of its compliance with the Privacy Rules. The FSU Dental Hygiene Clinic's policy is to maintain the required documentation for the required retention period.

Documenting the Policies and Procedures and the Notice of Privacy Practices. The Privacy Officer shall maintain a copy of the Policies and Procedures and the Notice of Privacy Practices for seven years beyond the date the documents cease to be effective.

Documenting Disclosures of PHI for Purposes of Responding to Requests for an Accounting. The Privacy Rules require that certain uses and disclosures be documented so that the FSU Dental Hygiene Clinic can respond to an individual's request for an accounting of disclosures (see section IV. C).

The FSU Dental Hygiene Clinic's policy is to require proper documentation of uses and disclosures of PHI, as required by the Privacy Rules. The Privacy Officer shall securely maintain the *PHI*

Disclosure Tracking Forms. Each form will be maintained for seven years beyond the date of the most recent entry on the form. The Privacy Officer will record on the PHI Disclosure Tracking Forms, at a minimum, the following information about disclosures of PHI:

- the individual whose PHI the FSU Dental Hygiene Clinic is disclosing
- the date of the disclosure
- the name of the entity or person who receives the PHI and, if known, the address of such entity or person
- a brief description of the PHI disclosed
- a brief statement of the purpose of the disclosure Uses and

Disclosures that Must Be Documented. The following disclosures of PHI must be documented for purposes of an accounting:

- all unauthorized disclosures known to the FSU Dental Hygiene Clinic
- disclosures to law enforcement
- disclosures to the Department of Health and Human Services
- any disclosures required by law, including those made:
    - in response to the order of a court or an administration tribunal
    - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, provided that there is an appropriate protective order in place and, where medical records are involved, the individual has waived his or her physician-patient privilege
    - pursuant to process (such as a court-ordered warrant or an administrative summons), and as otherwise required by law
- any of the following permitted disclosures:
    - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on the FSU Dental Hygiene Clinic' premises
    - about an individual that the FSU Dental Hygiene Clinic reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information
    - to appropriate public health authorities for public health activities

  - to a health oversight agency for health oversight activities
  - to coroners, medical examiners, and funeral directors about a deceased individual
  - for certain research purposes, when the need for an authorization has been waived or is otherwise not required
  - in order to avert serious threat to health or safety o about armed forces personnel to appropriate military command authorities
  - for protective services to the President of the United States and other designated persons
  - to correctional institutions and law enforcement custodians

Uses and Disclosures that Need Not Be Documented. The following uses and disclosures do not need to be documented for purposes of an accounting:

- to carry out treatment, payment and dental hygiene care
- to the individual that is the subject of the PHI (except formal requests to inspect and/or copy – see "Documenting Authorizations and Individual Rights" below)
- uses and disclosures incidental to permitted uses and disclosures
- pursuant to a valid authorization signed by the individual who is the subject of the use or disclosure
- for national security or intelligence purposes
- to correctional institutions or law enforcement custodians when the disclosure was permitted without an authorization
- uses and disclosures made as part of a limited data set

Documenting Authorizations and Individual Rights. The Privacy Officer shall securely maintain for a period of seven years from the date the document was last effective, the following:

- individual authorizations for the disclosure of PHI
- each request for an accounting of disclosures and all accountings related communications in response to the request.
- temporary suspensions of an individual's right to an accounting by:
  - a health oversight agency conducting health oversight activities authorized by law and described in the Privacy Rules

    - a law enforcement official, conducting an activity described in the Privacy Rules
- each request for confidential communications and all documents relating to the response to each
- each request to inspect and copy all documents related to the response to each
- each request to amend PHI and all documents relating to the disposition of each, if the FSU Dental Hygiene Clinic elects to amend the PHI, the amendment must be maintained with the record for as long as the record is maintained if the Dental Hygiene Clinic elects not to amend the request, the denial, and any statement of disagreement and rebuttal statement must also be kept with the record for as long as the record is maintained
- each request for additional restrictions and documents relating to the disposition of each
- an individual's agreement to receive a Notice of Privacy Practices by e-mail, and any withdrawal of such agreement

The obligation to retain documents relating to individual rights is limited to requests made to the FSU Dental Hygiene Clinic for documents maintained by the FSU Dental Hygiene Clinic. When PHI is held by a business associate, the individual will be referred to the business associate and the business associate is responsible for maintaining required documentation relating to individual rights.

In addition to the documents listed above, UEC may at its discretion maintain any additional documents it believes are appropriate relating to requests by individuals to exercise their individual rights under HIPAA.

Documenting Training. The Privacy Officer shall maintain documentation demonstrating the dates when employees with access to PHI were trained concerning the Privacy Rules and any applicable Policies and Procedures, for a period of seven years from the date the training was last effective.

Documenting Complaints. The Privacy Officer shall securely maintain documentation of all complaints that the FSU Dental Hygiene Clinic receives of violations of these Policies and Procedures or the Privacy Rules, and all documentation relating to disposition of the complaints. The FSU Dental Hygiene Clinic's will maintain these documents for seven years from the date of a complaint's final disposition.

Documenting Disciplinary Action. The Privacy Officer shall securely maintain documentation of all disciplinary action that the FSU Dental Hygiene Clinic has taken against employees for violations of these Policies and Procedures or the Privacy Rules, for a period of seven years from the date of the disciplinary action.

Documenting Mitigation Efforts. The Privacy Officer shall securely maintain all documents relating to the FSU Dental Hygiene Clinic's efforts to minimize the harmful effects of any unauthorized use or disclosure of an individual's PHI, for a period of seven years from the date of the action. Such documentation shall include known details of the unauthorized use or disclosure, details of the FSU Dental Hygiene Clinic's efforts to retrieve PHI or halt the improper use or disclosure, and all correspondence relating to the unauthorized use or disclosure.

Documenting Business Associate Agreements. The Privacy Officer shall maintain copies of all business associate agreements for a period of seven years from the date the contract was last in effect.

Documenting Breach Notifications. The Privacy Officer shall maintain copies of all notifications sent either on the FSU Dental Hygiene Clinic's behalf through its business associates or directly from the FSU Dental Hygiene Clinic to an individual in response to an unauthorized disclosure of PHI for a period of seven years from the date of notification.

N. Mitigation of Inadvertent Disclosures of PHI

1. *Generally*. The Privacy Rules require that the FSU Dental Hygiene Clinic minimize as much as possible any harmful effects resulting from an unauthorized use or disclosure of PHI. Policy is that all unauthorized uses or disclosures that come to the FSU Dental Hygiene Clinic's attention must be reported to the Privacy Officer so that the FSU Dental Hygiene Clinic may try to minimize any harmful effects of the unauthorized use or disclosure.

   An FSU Dental Hygiene Clinic employee who becomes aware of a use or disclosure of PHI, whether by an employee of the Dental Hygiene Clinic, a business associate, an outside consultant/contractor, or anyone else, that is not in compliance with these Policies and Procedures must do the following:

   - determine if there are steps that should be taken immediately to prevent any further potential harm to individuals whose PHI is involved in the unauthorized use and take reasonable

and appropriate action to prevent further potential harm, including immediate notification to the Privacy Officer of the unauthorized use or disclosure. The Privacy Officer may consult as necessary with legal counsel

- document the known details of the unauthorized use or disclosure for purposes of responding to a request for an accounting of disclosures (see section IV. C)
- follow any other instructions given by the Privacy Officer to minimize any harm resulting from the use or disclosure
    - if appropriate, follow the Breach Notification Requirements, below
    - evaluate current policies and procedures to determine whether modifications are appropriate
- document all efforts to minimize the harmful effects of the unauthorized use or disclosure in accordance with the Privacy Rules' documentation requirements (see section III. M)

2. *Breach Notification Requirements*. In the event of a potential breach of protected health/dental information, the FSU Dental Hygiene Clinic will investigate the incident. If the incident involves electronic PHI, the investigation will be consistent with the FSU Dental Hygiene Clinic's security incident investigation procedures. One or more members of the Breach Notification Team will participate in such investigation, when practical, 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 or consultants reasonably necessary to determine whether the FSU Dental Hygiene Clinic has a duty to notify individuals about a breach.

    A. Breach Notification Team In the event that the FSU Dental Hygiene Clinic learns that a breach may have occurred, breach, the FSU Dental Hygiene Clinic will establish a Breach Notification Team, which may consist of the following members, as appropriate:
        - Privacy Officer
        - Associate Dean of CHP
        - Security Officer
        - The FSU legal counsel/outside legal counsel
        - Upon request, any individual with knowledge or involvement in the specific incident

3. *Determining whether a breach has occurred* When the FSU Dental Hygiene Clinic learns of a possible breach, the Breach Notification Team must determine whether there has been an impermissible use or disclosure of unsecured protected health information under HIPAA's Privacy Rule. This includes situations in which a contractor/business associate notifies the FSU Dental Hygiene Clinic that an impermissible use or disclosure has or may have occurred. The following are examples of the types of situations that may need evaluation:
    - the FSU Dental Hygiene Clinic learns that an unauthorized individual has gained access to the FSU Dental Hygiene Clinic's electronic information system.
    - The FSU Dental Hygiene Clinic learns that an authorized individual may have accessed protected health information for an improper purpose.
    - The FSU Dental Hygiene Clinic learns that information intended for an authorized individual was misdirected (for example, by e-mail or fax transmission).
    - The FSU Dental Hygiene Clinic's learns that a business associate has suffered a potential data breach.
    - The FSU Dental Hygiene Clinic's hears from individuals who are the subject of the FSU Dental Hygiene Clinic's protected health information that they have been the victims of identity theft or other identity fraud crime.

    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 the FSU Dental Hygiene Clinic's HIPAA policies and procedures.
    - How the information was accessed, used or disclosed.

    i. 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.

    Note: while 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 the FSU Dental Hygiene Clinic has any obligations under state notification laws—whether or not notification is required under HIPAA.

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

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. The FSU Dental Hygiene Clinic 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 FSU Dental Hygiene Clinic determines, after an investigation, that there is a low probability that the information has been compromised, as described below.

4. *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:
        - The data has been properly encrypted consistent with guidance issued by the Department of Health & Human Services. This 35 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 email or structured electronic interchange), the encryption process must comply, as appropriate, with one of the following:
        - National Institute of Standards & Technology Special Publication 800-52, Guidelines for the Selection and

Use of Transport Layer Security (TLS) Implementations;
    - 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.
- 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:
    - 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.)
    - 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 documentation must be retained for a period of at least seven years from the date the Team concludes its evaluation of the incident. The Privacy Officer is responsible for retaining the necessary documents.

5. *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 the FSU Dental Hygiene Clinic's workforce
- A member of a business associate's workforce
- A person acting under the authority of the FSU Dental Hygiene Clinic' or the FSU Dental Hygiene Clinic's business associate
- The individual who acquired, accessed or used the protected health information did so in good faith.
- The acquisition, access or use did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

1. Inadvertent internal disclosure of protected health information. This exception applies if all of the following are true:
    - The disclosure is made by an individual who is authorized to access protected health information
    - The disclosure is made to an individual who is authorized to access protected health information.
    - Both individuals work for the same organization, which may be one of the following:
        - the FSU Dental Hygiene Clinic
        - the FSU Dental Hygiene Clinic's business associate
        - An organized health care arrangement in which the FSU Dental Hygiene Clinic participates.
    - The disclosure did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.
2. Where the information would not be retained. This exception applies if all of the following are true:
    - The disclosure is made to an unauthorized individual.
    - The FSU Dental Hygiene Clinic 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 Privacy Officer must retain the documentation for a period of at least seven years from the date the Team concludes its evaluation of the incident.

6. *Determine the probability that the 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 the risk assessment that there is a low probability that the information has been compromised.

   Factors to consider include:
   - The nature and extent of the 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 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 information could be re-identified based on the context and the ability to link the information with other available information?
   - The unauthorized person who used the 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 the FSU Dental Hygiene Clinic 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 information was viewed or acquired?
     - Does a forensic analysis indicate that information on a lost computer was never accessed, viewed, acquired, transferred, or otherwise compromised?
   - The extent to which the risk to the information 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 information has been compromised.

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

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 the FSU Dental Hygiene Clinic has a duty to notify the FSU Dental Hygiene Clinic of the breach within 60 days, but it is the FSU Dental Hygiene Clinic's duty to provide notification to the individuals impacted by the breach. Moreover, if the business associate is considered the FSU Dental Hygiene Clinic's agent, the FSU Dental Hygiene Clinic 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.

To reduce the risk to the FSU Dental Hygiene Clinic of a HIPAA violation, the FSU Dental Hygiene Clinic will seek to include in its business associate agreements a provision that requires the business associate to notify the FSU Dental Hygiene Clinic within 30 days of discovery. When appropriate, and after reaching consensus with the business associate, the FSU Dental Hygiene Clinic may also include a provision in the business associate agreement allocating responsibility for notification between the FSU Dental Hygiene Clinic and business associate. When a business associate reports a potential breach to the FSU Dental Hygiene Clinic, the Breach Notification Team will work with the business associate to determine whether the incident requires notification. If the business associate hires any subcontractors, these special requirements should also be included in the business associate's contract with its subcontractors, if applicable.

7. *Notification* If the Breach Notification Team determines that the FSU Dental Hygiene Clinic must provide notification of the incident, the Team will prepare appropriate notification as required below.

8. *Notice to Individuals*. Under HIPAA, the FSU Dental Hygiene Clinic must provide notice to affected individuals without unreasonable delay, but no later than 60 days after the date the FSU Dental Hygiene Clinic discovers the breach or should have discovered the breach if it had exercised appropriate diligence. To reduce the risk of exceeding the deadline, the FSU Dental Hygiene Clinic 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 individuals should take to protect themselves from potential harm resulting from the breach.
   - A brief description of what the FSU Dental Hygiene Clinic 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 the FSU Dental Hygiene Clinic knows that an individual is deceased and has the address of the deceased's next of kin or personal representative, the FSU Dental Hygiene Clinic may send the written notification to either next of kin or the personal representative.

   Under HIPAA, the FSU Dental Hygiene Clinic has no more than 60 days after discovery of the disclosure to notify individuals (though disclosure must be made earlier than 60 days if the FSU Dental Hygiene Clinic can reasonably do so). The date of discovery is measured as follows:
   - First day the breach is known to a member of the FSU Dental Hygiene Clinic's workforce or agents;
     - workforce member includes any employee, partner, volunteer, trainee, agent, etc.

- First day a member of the FSU Dental Hygiene Clinic workforce or its agents **would have known** of the breach by exercising reasonable diligence; or
- First day that the FSU Dental Hygiene Clinic 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 the FSU Dental Hygiene Clinic does not have sufficient contact information for some or all of the affected individuals (or if the contact information is outdated) then the FSU Dental Hygiene Clinic 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 the FSU Dental Hygiene Clinic'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 the elements required for the standard notice described above.
    - Substitute notice is not required in situations where an individual is deceased, and the FSU Dental Hygiene Clinic does not have sufficient contact information for the deceased individual's next of kin or personal representative.

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

The FSU Dental Hygiene Clinic's must retain copies of all notifications for at least seven years from the date the notifications were provided. For substitute notifications, retain copies for at least seven years from the date the notification was last posted on the website or the date the notification last ran in print or broadcast media. The Privacy Officer is responsible for retaining these documents.

9. *Notice to the Media*. If the Breach Notification Team determines that notification is required to more than 500 residents of a state, the FSU Dental Hygiene Clinic 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 the FSU Dental Hygiene Clinic'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.

   The FSU Dental Hygiene Clinic must retain copies of all press releases provided to prominent media outlets for at least seven years from the date the notifications were provided. The Privacy Officer is responsible for retaining these documents.

10. *Notice to the Department of Health & Human Services*. If the Breach Notification Team determines that the FSU Dental Hygiene Clinic or its business associate must provide notification to individuals under HIPAA, then the FSU Dental Hygiene Clinic's 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), the FSU Dental Hygiene Clinic 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:
    - The Privacy Officer 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.
    - The Privacy Officer 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 seven years from the date submitted to the Department. The Privacy Officer will retain the necessary documentation.

IV. Procedures for Complying with Individual Rights

The Privacy Rules give to individuals certain rights concerning their PHI that the FSU Dental Hygiene Clinic (or its business associates) maintains in a designated record set in connection with the Dental Hygiene Clinic. Individuals have the right to (1) inspect and copy their PHI, (2) request correction of their PHI, (3) receive an accounting of certain uses and disclosures of their PHI, (4) request confidential communication of their PHI, and (5) request additional protection for their PHI. The FSU Dental Hygiene Clinic's policy is to allow individuals to fully exercise their rights under the Privacy Rules.

Information about individuals covered by the Dental Hygiene Clinic is found in Dental Hygiene Clinic records maintained by the FSU Dental Hygiene Clinic and in records maintained by insurers and third-party administrators or other business associates involved in the administration of dental hygiene care. The FSU Dental Hygiene Clinic will respond to individual requests relating to records that it maintains. An individual seeking to exercise his or her individual rights with respect to records held by the Dental Hygiene Clinic's insurers or business associates will be directed to submit his or her request directly to the insurer or business associate with the relevant records. If an individual reports that an insurer or third-party administrator has not properly handled the request, the HIPAA Compliance Officer will

investigate the report under the Complaint procedures (see section II. D, beginning at page 7).

When the FSU Dental Hygiene Clinic receives a request for the information that it maintains, the FSU Dental Hygiene Clinic's will respond to the request using the following procedures.

A. Individual's Request to Inspect and Copy

The Privacy Rules give individuals the right to inspect and copy the records that the Dental Hygiene Clinic maintains about them in a designated record set. The FSU Dental Hygiene Clinic's policy is that all individuals will be given access to their designated record set, as required by the Privacy Rules (see 45 CFR 164.524).

The FSU Dental Hygiene Clinic's shall respond to requests for access by an individual, the parent of a minor child, or a personal representative using the following procedures:

- have the individual who requests access complete the FSU Dental Hygiene Clinic's Request to Inspect and Copy form
- verify the identity of the individual (or parent or personal representative) using the procedures set forth above under "Verifying the Identity of Those Requesting PHI" (see section III. L)
- document the request on the *Inspect and Copy Tracking Form*
- review the requested disclosure to determine whether the PHI requested is held in the individual's designated record set
    - if it appears that the PHI is not maintained in the individual's designated record set, contact the Privacy Officer
    - no request for access may be denied without the approval of the Privacy Officer
- review the requested disclosure to determine whether an exception exists that limits the individual's access to the requested PHI
    - the Privacy Rules specify that the following information need not be provided to the individual, and that grounds for denial are not reviewable:
        - psychotherapy notes
        - information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
        - health information about the individual that was collected from a third party under a promise of confidentiality

        - information maintained by certain clinical laboratories
        - certain health records held by or for correctional institutions about an inmate
        - information compiled during the course of research where the individual has agreed in advance to the denial of access until the research is completed
    - the Privacy Rules also allow information to be withheld under the following circumstances, but with a right by the individual to request a review of the decision:
        - a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person
        - the PHI makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that other person
        - the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual
    - if there is a question as to whether any restriction or exception applies, contact the Privacy Officer
    - no request for access may be denied without the approval of the Privacy Officer
- respond to the request on a timely basis:
    - Privacy Rule response deadlines:
        - if the records are maintained on site, the response is due within 30 days of the request
        - if the records cannot be accessed within the response time:
- the deadline can be extended 30 days by sending to the individual the FSU Dental Hygiene Clinic's 30-Day Extension Letter explaining the need for an extension of time
- the letter must be sent within the original 30-day deadline
    - enter response dates into docket or tickler system

- *Requests that Are Denied*. If the request to inspect and copy is denied:
    - the denial must be approved by the Privacy Officer
    - the denial must contain the following information provided on the *Inspect and Copy: Denial Letter*:
        - the basis for the denial
        - if applicable, a statement of the individual's right to have the decision to deny access reviewed
            - the statement must include an explanation of how the individual may seek review of the decision to deny access
            - if the individual seeks a review:
                - provide the *Individual Complaint Form* on which the individual may request a review
                - the decision must be timely reviewed by a licensed health care professional who was not originally involved in the decision to deny access ("reviewing official"); the FSU Dental Hygiene Clinic may designate who will serve as the reviewing official
                - the *Inspect and Copy: Review of Denial Letter* must be promptly sent to the individual to notify him or her of the reviewing official's determination
                - the FSU Dental Hygiene Clinic must take any other action required by the reviewing official
        - a description of how the individual may complain to the FSU Dental Hygiene Clinic or to HHS, including the name, title and telephone number of the Privacy Officer
    - if the denial only applies to a portion of the PHI being requested, then the rest of the information must be provided to the individual

- *Requests that Are Granted*. If the request is granted in whole or in part:
    - send the individual the Inspect and Copy: Grant Letter
    - the individual must be given access to the designated record set:
        - the individual has the right to inspect the record and to have a copy made
        - if the same PHI is maintained in more than one designated record set, or in more than one

location, the individual need only be given the information once in response to the request for access

- the individual has the right to designate a certain form of access (e.g., electronic form, paper form, in person, etc.)
  - if the individual has requested the PHI in a particular format (e.g., electronic file), the information should be provided in that format if it is readily producible in that format
  - otherwise, produce the information in readable hard copy form or in such other form as the individual agrees to receive
  - if the PHI is in coded form, an accurate translation in plain English must be provided

- *Providing a Summary*. Summary or explanation of PHI in lieu of access to record:
  - in lieu of providing access to the record, or in addition to the full record, the FSU Dental Hygiene Clinic may provide the individual with a summary or explanation of the information, if the individual:
    - agrees in advance to receive the summary or explanation
    - agrees in advance to pay any fees that may be imposed for the summary or explanation
  - if an individual agrees to accept a summary or explanation and any associated fees:
    - prepare the summary or explanation
    - provide the information in the requested format

- *Charging Reasonable Fees*. The FSU Dental Hygiene Clinic may charge the following fees for access to the records:
  - the FSU Dental Hygiene Clinic's may not charge for retrieving or handling the information o if photocopies are requested:
    - the FSU Dental Hygiene Clinic's may charge for the costs of supplies used in making the copies, including the cost of the paper
    - the FSU Dental Hygiene Clinic's may charge for the time the Dental Clinic Clerk spends on making the copies at the employee's hourly rate. If the employee is a salaried employee, a pro rata hourly rate must be calculated to determine the charge

    - if the information is provided on a computer disk or other portable electronic media, the FSU Dental Hygiene Clinic may charge for the cost of the media
    - if the request is to have the records sent by mail or other type of delivery service (such as UPS, Federal Express, etc.), the FSU Dental Hygiene Clinic may charge for the actual cost of the postage or delivery service requested
    - if the request is for a summary or explanation of the individual's records, the FSU Dental Hygiene Clinic may charge for the time the FSU Dental Hygiene Clinic spent preparing the summary or explanation at the employee's hourly rate. If the employee is a salaried employee, a pro rata hourly rate must be calculated to determine the charge
- if the disclosure is made to the parent of a minor or a personal representative, document the disclosure according to the documentation requirements (see section III. M)
- If the FSU Dental Hygiene Clinic maintains the information in an electronic form, the FSU Dental Hygiene Clinic must be able to provide the information in an electronic form to an individual. The FSU Dental Hygiene Clinic must provide the individual with access to the information in the electronic format requested by the individual if it is readily producible in that format. If the FSU Dental Hygiene Clinic cannot provide the information in the requested format, it will offer to produce the information in the formats that are available. If the FSU Dental Hygiene Clinic and the individual cannot agree on an electronic format, the FSU Dental Hygiene Clinic may produce the records in paper form.
- If an individual's request for access directs the FSU Dental Hygiene Clinic to transmit a copy of the information to another person designated by the individual, the FSU Dental Hygiene Clinic must provide a copy to the person designated by the individual. The individual's request must be: (1) in writing (2) signed by the individual; (3) clearly identify the designated person; and (4) clearly identify where to send the copy of information. The request does not need to comply with the Authorization requirements.

B. Individual's Request for Amendment

The Privacy Rules give individuals the right to request an amendment of their records that the Dental Hygiene Clinic maintains in a designated record set. The FSU Dental Hygiene

Clinic's policy is that individuals will be given the right to request an amendment of their designated record set as required by the Privacy Rules.

The FSU Dental Hygiene Clinic's shall respond to the request to amend the record made by an individual, the parent of a minor child, or a personal representative using the following procedures:

- have the individual complete the FSU Dental Hygiene Clinic's Request to Amend form
- verify the identity of the individual (or parent or personal representative) using the procedures set forth above under "Verifying the Identity of Those Requesting PHI" (see section III. L)
- record the request on the *Amendment Request Tracking Form*
- review the requested disclosure to determine whether the PHI to be amended is held in the individual's designated record set
    - if it appears that the PHI is not maintained in the individual's designated record set, contact the Privacy Officer
    - no request for access may be denied without the approval of the Privacy Officer
- review the requested amendment to determine whether the individual would have access to the PHI to be amended under the individual's right to inspect and copy, following the procedures set forth in Individual's Request to Inspect and Copy" (see section IV. A)
- respond to the request on a timely basis:
    - Privacy Rule deadlines:
        - a written response informing the individual whether the request is being denied or granted is due within 60 days of the request
        - if the determination cannot be made within 60 days:
            - the deadline can be extended by 30 days by sending the individual the FSU Dental Hygiene Clinic *30-Day Extension Letter* explaining the need for an extension of time
            - the letter must be sent within the original 60-day deadline
            - enter response date into docket or tickler system
- *Requests that Are Granted*. If the request for an amendment is approved:

- send the individual the *Amendment: Grant Letter*
- make the change in the designated record set. Any records affected must be appended or a link must be provided to the location of the amendment
- provide notice to the individual and any additional persons or entities listed on the individual's *Request to Amend* form
- provide notice to any persons/entities known to have the particular record and who may rely on the uncorrected information to the detriment of the individual. Other designated record sets are typically maintained by:
  - third party administrators

- *Requests that Are Denied*. If the request for an amendment is denied, in whole or in part:
  - the denial must be approved by the Privacy Officer
  - the denial must be in writing using the FSU Dental Hygiene Clinic *Amendment: Denial Letter* denying the individual's request for amendment of PHI, setting forth the following information:
    - *The basis for denial*. The appropriate reasons for denying the amendment are:
      - the record or PHI was not created by the FSU Dental Hygiene Clinic
      - the record or PHI is not part of the designated record set
      - the record or PHI is not accessible to the individual under the individual's right to inspect and copy
      - the record is already accurate and complete
    - *Explanation of Right to Submit Disagreement*. An explanation of the individual's right to submit a written statement disagreeing with the denial, with instructions on how to file such a statement
      - the written statement shall by submitted on the FSU Dental Hygiene Clinic *Statement of Disagreement Form*
      - the FSU Dental Hygiene Clinic may prepare a rebuttal to the individual's written statement, which shall be prepared using the FSU Dental Hygiene Clinic Rebuttal to *Statement of Disagreement Form*, a copy of which must be provided to the individual

- an explanation that if the individual does not submit a *Statement of Disagreement Form*, he or she may request that any future disclosures of the PHI that is the subject of the request for amendment include the request for amendment and the denial
- a description of how the individual may complain to the FSU Dental Hygiene Clinic or to HHS, including the name, title and telephone number of the Privacy Officer

- the individual's record must be updated to reflect the request for amendment and denial:
  - identify the PHI or record that is the subject of the request for amendment
  - append to or otherwise link the PHI or record with the following:
    - the individual's *Request to Amend*
    - the FSU Dental Hygiene Clinic *Amendment: Denial Letter*
    - the individual's *Statement of Disagreement* (if submitted)
    - the FSU Dental Hygiene Clinic *Rebuttal to Statement of Disagreement* (if prepared)
    - all future disclosures of the PHI or record must include the following:
      - if the individual filed a *Statement of Disagreement*, include with the disclosure:
      - the individual *Request to Amend*
      - the FSU Dental Hygiene Clinic *Amendment: Denial Letter*
      - the individual's *Statement of Disagreement* (if submitted)
      - the FSU Dental Hygiene Clinic *Rebuttal to Statement of Disagreement* (if prepared)
    - if the individual did not file *a Statement of Disagreement*, include the individual's *Request to Amend and the Amendment*: *Denial Letter* with the record, if the individual has requested such action
    - if the PHI or record is being transmitted electronically as part of a standard

transaction, the FSU Dental Hygiene Clinic may separately transmit the documents noted above to the recipient of the standard transaction

- if the FSU Dental Hygiene Clinic receives notification from another covered entity of an amendment to the individual's PHI, will amend the PHI in the individual's designated record set by appending or otherwise linking the amended information to the location of the amendment

C. Individual's Request for an Accounting of Disclosures of PHI

The Privacy Rules give individuals the right to request an accounting of disclosures of their PHI. the FSU Dental Hygiene Clinic's policy is to respond to such requests as required by the Privacy Rules.

The FSU Dental Hygiene Clinic shall respond to a request for an accounting made by an individual, the parent of a minor child, or a personal representative using the following procedures:

- have the individual complete the FSU Dental Hygiene Clinic *Request for an Accounting of Disclosures form*
- verify the identity of the individual (or parent or personal representative) using the procedures set forth above under "Verifying the Identity of Those Requesting PHI" (see section III. L)
- record the request on the *Disclosures Requests Tracking Form*
- determine whether the individual has previously requested an accounting
    - the Privacy Rules require the FSU Dental Hygiene Clinic to provide one accounting to an individual in any 12-month period without a charge. the FSU Dental Hygiene Clinic's policy is to provide two accountings to an individual in any 12-month period without a charge
    - if the individual has made two requests within the 12 months prior to the date of the current request:
        - the FSU Dental Hygiene Clinic may charge for its actual costs in responding to the request
            - the charge may not include a charge for retrieving or handling the information
            - the FSU Dental Hygiene Clinic may charge for the time the FSU Dental Hygiene Clinic spends preparing the accounting at the employee's hourly rate. If the employee is a

salaried employee, a pro rata hourly rate must be calculated to determine the charge
        - provide individual with the *Accounting of Disclosures Letter* informing him or her:
            - the fee that will be charged for the additional accounting
            - that the individual may withdraw or modify the request to avoid or reduce the fee
- determine whether there has been a temporary suspension imposed on the individual's right to an accounting
    - a health oversight agency or law enforcement official, in appropriate circumstances, may suspend an individual's right to an accounting if the accounting would impede the agency's activities
    - if a suspension has been documented, contact the Privacy Officer for guidance
- respond to the request for an accounting on a timely basis: o a written response is due within 60 days that either:
    - provides the accounting; or
    - informs the individual that there have been no disclosures that must be included in the accounting
    - enter response dates into docket or tickler system
    - if the accounting cannot be provided within 60 days:
        - the deadline can be extended 30 days by sending to the individual the FSU Dental Hygiene Clinic *30-Day Extension Letter* explaining the need for an extension of time
        - the letter must be sent within the original 60-day deadline
- in preparing the accounting, include disclosures following these guidelines:
    - include all disclosures (but not uses) of the requesting individual's PHI made by the and any of its business associates during the period seven years prior to the date of the request
    - the accounting does not have to include disclosures made:
        - to carry out treatment, payment, or health care operations
        - to the individual who is the subject of the PHI
        - incident to an otherwise permitted use or disclosure
        - pursuant to the individual's authorization

        - for specific national security or intelligence purposes
        - to correctional institutions or law enforcement custodians when the disclosure was permitted without an authorization
        - as part of a limited data set
- determine whether accounting information must be obtained from business associates o review contracts with business associates to determine which business associates have authority to disclose the individual's PHI
    - contact business associates with authority to disclose PHI to request the information necessary to respond to the accounting
        - follow contractual provisions for providing notice to business associate of individual's request for accounting
        - pursue contacts by phone to monitor the status of business associates' response to the request
- for each reportable disclosure, provide the following information:
    - the date of the disclosure
    - the name and, if known, the address of the entity or person who received the PHI
    - a brief description of the PHI disclosed
    - the reason for the disclosure, which may be in the form of:
        - a brief statement of the reason for the disclosure that reasonably informs the individual of the basis for the disclosure; or
        - if applicable, a copy of a written request for the disclosure when the disclosure was:
            - in response to a request from HHS
            - one of the permitted disclosures of PHI for legal and public policy purposes
    - if during the accounting time period the FSU Dental Hygiene Clinic has made multiple disclosures of the individual's PHI to the same person or entity for a single purpose, these multiple disclosures may be accounted for as follows:
        - for the first disclosure, provide all of the details listed above
        - for the subsequent disclosures, provide:

- the frequency, periodicity, or number of disclosures made during the accounting period; and
- the date of the last such disclosure during the accounting period

- document the disclosure according to the Privacy Rules' documentation requirements (see section III. M).

D. Individual's Request for Confidential Communications

The Privacy Rules give individuals the right to request confidential communications, which must be accommodated when reasonable. The FSU Dental Hygiene Clinic policy is to accommodate all reasonable requests for confidential communications as required by the Privacy Rules.

The FSU Dental Hygiene Clinic shall respond to a request for confidential communications from an individual, the parent of a minor child, or a personal representative using the following procedures:

- have the individual complete the FSU Dental Hygiene Clinic *Request for Confidential Communications form* and determine how the individual prefers to be contacted with respect to the decision of whether to grant or deny the request
  - the employee accepting the *Request for Confidential Communications* may not request an explanation from the individual as to the basis for the request for confidential communications
- verify the identity of the individual (or parent or personal representative) using the procedures set forth above under "Verifying the Identity of Those Requesting PHI" (see section III. L)
- determine whether to accommodate the request:
  - if the individual has indicated that disclosure of all or part of the information to which the request pertains could endanger the individual:
    - the FSU Dental Hygiene Clinic policy is to accommodate the request whenever reasonable, and Privacy Officer must be involved in any decision to deny the request
    - if the individual's request, as stated, cannot be accommodated, the individual should be contacted in person, in writing, or by telephone to explain why the request cannot be accommodated

and to determine if an alternate arrangement for confidential communications can be worked out
        - if anything is unclear about the instructions for confidential communications, the individual must be promptly contacted in person, in writing or by telephone in order to clarify the instructions
        - inform the individual whether the request is being granted or not o if the request does not indicate that disclosure of all or part of the information to which the request pertains could endanger the individual:
    - it is the FSU Dental Hygiene Clinic policy to accommodate the request whenever reasonable. the FSU Dental Hygiene Clinic will consider the nature of the request and the difficulty of complying with the request
        - if the individual's request, as stated, cannot be accommodated, the individual should be contacted in person, in writing, or by telephone to explain why the request cannot be accommodated and to determine if an alternate arrangement for confidential communications can be worked out
        - if anything is unclear about the instructions for confidential communications, the individual should be promptly contacted in order to clarify the instructions
        - notify the individual to indicate whether the request is being granted or not
- if a request for confidential communications is approved:
    - promptly update the information in the individual's benefit file to indicate that confidential communications must be delivered by the designated alternate means
    - promptly update the individual's contact information on the FSU Dental Hygiene Clinic's electronic data system to indicate that communications to the individual must be delivered by the designated alternate means
    - promptly notify and convey to any relevant third-party administrator(s) the request for alternative communications with instructions for the third party administrator(s) to update their records
    - promptly notify and convey the request to any other third parties known to maintain records and communicate with the individual the request for confidential communications

- requests and their dispositions must be documented according to the Privacy Rules' documentation requirements (see section III. M).

E. Individual's Request for Restrictions on Uses and Disclosures of PHI

The Privacy Rules give individuals their right to request that the FSU Dental Hygiene Clinic's restrict its uses or disclosures of their PHI beyond the restrictions imposed by the Privacy Rules. The Privacy Rules do not require the FSU Dental Hygiene Clinic's to agree to any requested restrictions.

The FSU Dental Hygiene Clinic's policy is to permit an individual to request restrictions on uses and disclosures as required by the Privacy Rules. the FSU Dental Hygiene Clinic's shall respond to a request for restrictions on uses and disclosures of PHI by an individual, a parent of a minor child, or a personal representative using the following procedures:

- have the individual complete the FSU Dental Hygiene Clinic Request for Additional Restrictions form
- verify the identity of the individual (or parent or personal representative) using the procedures set forth above under "Verifying the Identity of Those Requesting PHI" (see section III. L)
- the FSU Dental Hygiene Clinic policy is that requests for additional restrictions are generally not granted because of the additional administrative burden associated with such additional restrictions. If such a request is granted, it will be granted only by the Privacy Officer, after a determination that (1) there are no additional administrative burdens associated with the request, (2) the circumstances otherwise warrant a departure from the FSU Dental Hygiene Clinic normal policy, or (3) the request is accompanied by a court order requiring the restriction (such as a protective order)
- respond to the *Request for Additional Restrictions* by using the FSU Dental Hygiene Clinic form letter
- if a request for additional restrictions is approved: o update the information in the individual's benefit file to indicate the additional restrictions associated with the individual
    - update the individual's information on the FSU Dental Hygiene Clinic electronic data system to indicate the additional restrictions that apply

    - convey to any relevant third-party administrator the additional restrictions with instructions for the third party administrator to update its records
    - promptly notify and convey to any other third parties known to use the individual's PHI the additional restrictions
- requests and their dispositions must be documented according to the documentation requirements (see section III. M).

V. Minimum Necessary

Purpose

To make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

Policy

When possible, the minimum amount of information necessary should be "Limited Data Set" information. When additional information is needed, the Dental Hygiene Clinic will only use or disclose the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure under the conditions and exceptions described in this policy.

Procedure

1. People in the following job categories will only have access to the kind or amount of protected health information indicated:
    a. Workforce members including dental hygiene students - any and all protected health information, including the entire clinical chart, for treatment payment and health care operations.
    b. Dental clinic clerks and work studies - any and all protected health information needed to perform their job duties.

2. We will keep all clinical charts and billing records secure when they are not in use. Paper records will be locked in files behind locked doors. Only authorized staff will have access to this secure storage. All staff is prohibited from browsing at someone else's workstation or using their computer

password. Staff is prohibited from talking about patients in public areas.

3. All staff will sign a "confidentiality agreement" indicating their commitment to access only the minimum amount of protected health information necessary for them to do their job, and to abide by the restrictions listed in paragraph 2. Violation of this agreement is grounds for employee discipline according to our personnel policies.

4. Whenever we get a request from a third-party for protected health information about one of our patients, or whenever we intend to make a unilateral disclosure of protected health information about one of our patients, we will disclose only the minimum amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:
    a. The patient has authorized the disclosure.
    b. The disclosure is for treatment purposes payment, or health care operations (for example, disclosures to a consultant or follow-up health care provider).
5. We will rely upon the representations of the following third parties that they have requested only the minimum amount of protected health information necessary for their purposes:
    a. Another health care provider or health plan.
    b. A public official, like a law enforcement officer.
    c. Professionals providing services to us (such as attorneys or accountants).
6. The Privacy Officer is responsible for determining what is the minimum amount of protected health information necessary for us to disclose in situations that are not routine. The Privacy Officer will consider the reason for the disclosure, whether it falls into any of the circumstances described in paragraph 4 of this policy, and the protected health information that we have, in making this determination.
7. Whenever we request protected health information about one of our patients from someone else, we *will* ask for only the minimum necessary amount of protected health information

necessary for us to accomplish the purpose that prompted us to ask for the information.

8. Electronic Medical Records are only accessible by specific permissions granted to individual staff based upon the minimum necessary for them to complete their job duties.

Exceptions to the Minimum Necessary Standard

The minimum necessary standard does not apply to:

- disclosures to a health care provider for treatment
- disclosures to the individual who is the subject of the PHI
- uses or disclosures made pursuant to an authorization • disclosures made to HHS
- disclosures about victims of abuse, neglect or domestic violence, when required by law
- uses or disclosures in response to the order of a court or administrative tribunal
- disclosures pursuant to process or as otherwise required by law
- uses or disclosures that are required for compliance with the Privacy Rules

VI. FUNDRAISING

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.

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

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 Associate Dean 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, temporary 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 Associate Dean.

- **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 ten 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.

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

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 _____.

Type of routine disclosure	**Patient information that may be disclosed without checking with the Privacy Officer**

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 _____.

Type of routine disclosure	**Patient information that may be disclosed without checking with the Privacy Officer**

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
COLLEGE OF HEALTH PROFESSIONS

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)

Name of patient(s) whose information you are requesting:
_____

Patient(s) Date of Birth: _____

The specific patient information you are requesting:
_____
_____
_____

Your Name: _____

Address: _____

City: _____ State: _____ Zip: _____

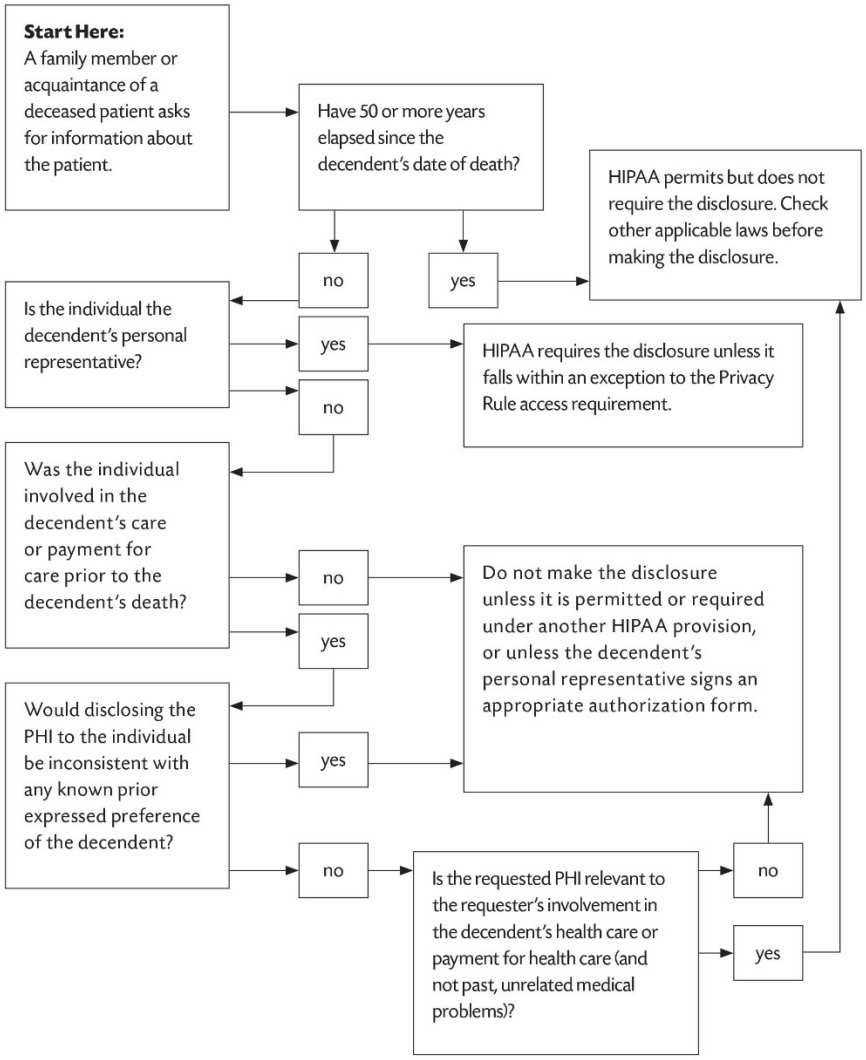
Describe your authority to access this information:
_____
_____

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:
_____

Sample Decision Tree: Decedent PHI



FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA AUTHORIZATION FORM FOR USE AND DISCLOSURE OF PATIENT INFORMATION USING CORE ELEMENTS 45 CFR 164.508

This form is for obtaining and documenting authorization for 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.

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA REQUEST FOR ACCESS FORM

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

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 $ _____.
- ☐ I want you to send the copy of the requested records to:

Name: _____

Address:_____

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: _____

Fees

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

Please contact our Privacy Officer if you have any questions about your privacy to inspect or copy records.

Privacy Officer:
DH Clinic Operations Supervisor or the Associate Dean of the College of Health Professions, Telephone: 231-591-2260

For Dental Office Use Only

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

- ☐ Request for access denied (attach written denial)
- ☐ Request for access approved

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA 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/ or Associate Dean of the College of Health Professions

Ferris State University, College of Health Professions, 200 Ferris Drive, Big Rapids, MI 49307 231-591-2260

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA DENIAL OF REQUEST TO AMEND FORM

Patient's Name:
Address:

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 or Associate Dean of the College of Health Professions
Ferris State University, 200 Ferris Drive, Big Rapids, MI 49307 231-591-2260

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

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.

PATIENT NAME	AMENDMENT REQUESTED	APPROVED OR DENIED?	DATE AMENDMENT COMPLETED	LIST 3RD PARTIES WHO MUST BE NOTIFIED OF THE AMENDMENT	DATE AMENDMENTS SENT TO 3RD PARTIES

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA LOG OF DISCLOSURES OF PATIENT INFORMATION

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.

Patient Name	Date of Disclosure	Who received the information?	Description of PHI disclosed	Purpose of disclosure	Was the disclosure for research?	Is this one of multiple disclosures that can be grouped?

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA 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 Information:

Print Name: _____
Patient DOB: _____ (For identification purposes)
Signature: _____

Date: _____

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: _____
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.

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA 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
COLLEGE OF HEALTH PROFESSIONS

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 items(s) and/or services(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 items(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 **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: _____

Privacy Officer or Associate Dean of the College Of Health Professions 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 pain in full (see Section A of this form).

Signature: _____Date: _____

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

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:

1.	Date the suspected breach was discovered?	
2.	Date the suspected breach occurred?	
3.	Describe with a brief statement of what happened.	
4.	How we learned of the breach.	
5.	Describe the people and entities involved.	
6.	Did the incident involved "use" of information?	
7.	Who used the information?	
8.	For what purpose was the information used?	
9.	If the incident involved a disclosure of information:	
10.	Who disclosed the information?	
11.	To whom?	
12.	For what purpose?	
13.	Describe the format of the information (paper chart, electronic, films)	

14.	If electronic information was involved:	
15.	Was the electronic information in storage? (On a desktop, computer hard drive, a laptop, a CD or a USB?)	
16.	Was the electronic information in transit? (mail or through a portal?)	
17.	Was the electronic information properly encrypted?	
18.	Was the password of an authorized person/entity used to access the information?	
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:

1.	Was the information properly "secured" using a method approved by the U.S. Dept. of HHS?	YES	NO
2.	If YES, explain:		
3.	Was the information PHI?	YES	NO
4.	If NO, explain:		
5.	Was the use or disclosure permitted or required? (Authorization forms required)	YES	NO

6.	Attach a copy of the signed authorization form(s)		
7.	Do any of the following EXCEPTIONS apply?		

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.

Does any one of these three exceptions apply?	YES	NO
If YES, explain:		

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? I 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 THE FSU DENTAL HYGIENE CLINIC 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.

Name: _____

Signed: _____ Date: _____

Title: _____ Date: _____

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

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:

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA AGREEMENT TO RECEIVE ELECTRONIC COMMUNICATION

Patient Name: _____ Date of Birth: _____

I agree that the Ferris State University Dental Hygiene Clinic l 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:

THE FSU DENTAL HYGIENE CLINIC 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: _____

FERRIS STATE UNIVERSITY
COLLEGE OF HEALTH PROFESSIONS

FERRIS STATE UNIVERSITY DENTAL HYGIENE
HIPAA COMPLAINT LOG FORM

Complaint	Name and contact information of the person making the complaint	Date complaint was made	Date response sent to person who made the complaint	Sanctions, if any

Describe any changes resulting from the complaint, i.e., training, Policy and Procedure redesign: