FERRIS STATE UNIVERSITY

University Eye Center

HIPAA

Privacy Compliance

Manual

02/20/2014

Table of Contents

Introduction

In enacting HIPAA in 1996, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. HIPAA compliments and supplements other state and federal confidentiality laws including health care professional licensing laws as well as other confidentiality policies of the University Eye Center (UEC) at the Michigan College of Optometry (MCO) and Ferris State University (FSU).

HIPAA, as it is reflected and applied in this policy, requires health care providers including UEC to implement various activities such as:

- Notifying patients about their privacy rights and how their information can be used.
- Securing patient records containing individually identifiable health information.
- Adopting and implementing privacy policies and procedures for its practice.
- Training employees so that they understand privacy procedures.
- Designating an individual within the practice to be responsible for seeing that the privacy procedures are adopted and followed.

On January 25, 2013, the federal government published changes to the HIPAA rules that require health care components of hybrid entities (such as the University Eye Center) to update compliance programs. The changes are effective March 26, 2013, but health care components have until September 23, 2013 to come into compliance. All business associate agreements entered into on or after January 25, 2013 must be compliant with the new requirements by September 23, 2013, but a transition period until September 22, 2014 applies to certain agreements that were in place on January 25, 2013.

Policy Statement

FERRIS STATE UNIVERSITY HAS DESIGNATED ITSELF AS A HIPAA HYBRID ENTITY, WITH THE UNIVERSITY EYE CENTER DESIGNATED AS A HEALTH CARE COMPONENT INCLUDED IN THE HYBRID ENTITY. UEC CONDUCTS CERTAIN FINANCIAL AND ADMINISTRATIVE TRANSACTIONS AND MEDICAL RECORDS ELECTRONICALLY, AND POSSESSES INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION. UEC WILL COMPLY WITH ALL OF THE REQUIREMENTS OF HIPAA'S PRIVACY RULE.

THE UNIVERSITY EYE CENTER WILL NOT DISCLOSE PROTECTED HEALTH INFORMATION TO NON-HEALTH CARE ENTITIES WITHOUT A SIGNED PATIENT AUTHORIZATION OR OTHER HIPAA PERMISSION. UEC WILL INSTITUTE APPROPRIATE SAFEGUARDS TO PREVENT IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION TO NON- HEALTH CARE ENTITIES.

Important Definitions and Concepts Used in These Policies and Procedures

Business Associate	A person or organization, other than a member of the UEC workforce, that creates, receives, maintains or transmits PHI on behalf of UEC. A business associate arranges, performs, or assists in the performance of functions or activities for the UEC that involve PHI. A business associate can also be a covered entity in its own right. Also see Part II, 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	Under HIPAA, this is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. Also see Part II, 45 CFR 160.103.
De-identified Information	Protected health information under HIPAA is *individually identifiable* health information. De-*Identifiable* data is data that has been stripped of any and 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)
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]
Designated Record Set	The Designated Record Set is defined as records (paper or electronic) maintained by or for UEC that are the medical and billing records about patients; or the enrollment, payment, claims adjudication, and case or medical management record systems; and/or used, in whole or in part, by UEC to make decisions about patients.
Healthcare 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 nonhealth-care 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	1) The activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) a health-care provider or health plan to obtain or provide reimbursement for the provision of health care; and 2) the activities relate to the individual to whom health care is provided and include, but are not limited to (i) determinations of eligibility or coverage and adjudication or subrogation of health benefit claims, (ii) risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance) and related health-care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (a) name and address; (b) date of birth; (c) social security number; (d) payment history; (e) account

	number; and (f) name and address of the health-care provider or health plan.
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. See Part II, 45 CFR 164.501.
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, UEC 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/Employee	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.

I. Responsibilities as a Covered Entity

1. Privacy Officer and Contact Person. A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

2. Workforce Training. A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule. Trainings will be recorded and maintained in the Privacy Officer's office employee record.

3. Safeguards. UEC maintains reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.
    a. Administrative Safeguards. Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
        i. Appointment of Privacy Officer & duties
        ii. Employee Training
        iii. Risk Assessment and Management
    b. Technical Safeguards. Technical safeguards are the technology and the policy and procedures for its use that protect Electronic Protected Health Information (ePHI) and control access to it.
        i. Email
        ii. Facsimile
        iii. Access controls
        iv. Emergency Access
        v. Automatic Log-off
    c. Physical Safeguards.
        i. Record Retention and Destruction
        ii. Laptops and iPads
        iii. Incidental Disclosures
        iv. Private check-in and check-out

4. Complaints. A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain those procedures in its privacy practices notice.

5. Discipline
    a. Type of Discipline. When protected health information is improperly accessed, used or released, an individual may be disciplined based on the individual's classification. The specific discipline administered will depend on the nature and severity of the violation.

Disciplinary action can range from a verbal warning to immediate termination of the employee.

b. Whistleblowers. HIPAA regulations permit workforce members of covered entities to disclose PHI in order to expose unlawful or unprofessional conduct, without concern for Intimidation or Retaliatory Acts. Whistleblower disclosures must be:

- based on a "good faith belief" that such unlawful of unprofessional conduct has occurred, and that disclosure of the PHI is necessary to revealing it;
- made to a health oversight agency, public health authority or other entity authorized by law to investigate such conduct (such as a law enforcement agency), or to an attorney retained for the purposes of determining legal options in the matter; and
- no more than reasonably necessary to establish the unlawful or unprofessional conduct (given that the minimum necessary standard can reasonably be inferred to cover all actions associated with PHI).

c. Crime Victims. UEC is not in violation of the rule when a workforce member of a covered entity who is the victim of a crime discloses protected health information to law enforcement officials about the suspected perpetrator of the crime.

6. No Intimidating or Retaliatory Acts. UEC 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.

7. No Waiver of Rights. UEC 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.

8. Notice of Privacy Practices. A covered entity under HIPAA must create and provide a Notice of Privacy Practices (NPP) to every patient.

   a. Creating the Notice.
   b. Delivering the Notice.
   c. Electronic Delivery of the Notice.
   d. Posting the Notice on UEC Website.
   e. Revisions of the NPP.

II. Uses and Disclosures of Protected Health Information.

1. Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either:

   a. as the Privacy Rule permits or requires; or

b. as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

2. Who Must Comply with These Policies and Procedures

Health Care Providers. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule. Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care. **UEC and Staff must comply with these policies and procedures.**

3. Minimum Necessary. A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must 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. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. When possible, the minimum amount of information necessary should be the Limited Data Set information.

Exceptions to the Minimum Necessary Standard. The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

4. Complying with Minimum Necessary.
    a. Access and Uses. For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

5. Required Disclosures**.** A covered entity must disclose protected health information in only two situations:

    a. to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information;

    b. to HHS when it is undertaking a compliance investigation or review or enforcement action.

6. Permitted Uses and Disclosures. A covered entity 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. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

7. Authorized Use and Disclosure. A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. A covered entity may not require conditions pursuant to treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.
    a. An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party.
    b. An authorization that is valid must specify a number of elements including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, a statement regarding the right a patient has to revoke the authorization, and, in some cases, the purpose for which the information may be used or disclosed.
    c. A patient has the right to revoke an authorization at any time. The revocation must be in writing, and is not effective until the covered entity receives it. In addition, a written revocation is not effective with respect to actions a covered entity took in reliance on a valid Authorization, or where the Authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.
    d. A patient has the right to receive a copy of their completed Authorization.
    e. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.
        i. Marketing. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value.

III. Complying with Individual Rights

Notice and Other Individual Rights

Privacy Practices Notice. Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.

Access**.** Except in certain circumstances, patients have the right to review and obtain a copy of their protected health information in a covered entity's designated record set. The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, a covered entity may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion. The covered entity may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Privacy Rule gives patients the right to have a covered entity amend their protected health information in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the patient has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. The covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

Disclosure Accounting. Patients have a right to an accounting of the disclosures of their protected health information by a covered entity or their Business Associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.

The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

Restriction Request. Patients have the right to request that covered entities restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. If a patient pays the full cost of treatment without any contribution from a health plan, the health care provider must agree, upon request, not to share the information treatment with the patient's health plan for payment or health care operations purposes. Except in limited circumstances, covered entities are under no obligation to agree to requests for restrictions.

Confidential Communications Requirements. Covered entities must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that we typically employs. For example, a patient may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card.

IV. Breach Notification

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Breach Notification Requirements. Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Privacy Policies and Procedures

University Eye Center

Ferris State University

Designation of a Privacy Officer

Purpose

To ensure that a designated individual is appointed / selected to serve as the primary contact and Privacy Officer for the purpose of carrying out HIPAA and Privacy Rule related duties and responsibilities.

Policy

UEC and General Counsel will designate a privacy officer responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

Procedure

1. The Clinic Operations Supervisor of UEC is the designated Privacy Officer.
2. The Privacy Officer may appoint a Designee.
3. The Privacy Officer is responsible for developing and implementing the UEC privacy policies and procedures, and designated as
    a. The person for receiving complaints
    b. Providing further information about the Notice of Privacy Practices (for example, to patients, to staff, etc.), and
    c. Receiving and processing:
        i. Requests for access
        ii. Accountings of disclosures
        iii. Requests for amendments

PRIVACY OFFICER JOB QUALIFICATIONS AND DESCRIPTION

In order to comply with HIPAA's Privacy Rule, this office will have a privacy officer.

1. Qualifications to serve as privacy officer:

- Knowledge of the HIPAA Privacy Rule.
- Available time to devote to compliance effort.
- Available time to attend educational seminars on privacy compliance, and to summarize seminar content for staff.
- Capable of sustained and detailed effort.
- Capable of effectuating change, when needed.
- Capable of creative or innovative solutions to privacy issues.
- Good communication skills.
- Good organizational skills.
- Motivates staff to achieve compliance.
- Prudent fiscal manager.
- Works well with governing body or management.
- Works well with outside resources, as applicable.

2. Duties of the privacy officer:

- **Management**
  Work with University General Counsel (GC) to comply with applicable federal and state laws. Stay current on privacy laws and updates in privacy technology. Immediately notify the direct Administrator 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 UEC 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, interns and others whose work for UEC is under the practice's direct control. Oversee sanctions for violations of HIPAA and our privacy policies and procedures according to our policies, and bring any sanctions to the attention of the direct Administrator.

- **Risk Management**
  Collaborate with appropriate University Security Official to ensure that privacy and security risks are assessed regularly and are analyzed, documented and updated as appropriate.

- **Business Associates**
  Ensure that appropriate agreements are in place with each of the UEC's business associates. Lead the practice in developing and updating business associate agreements and work with GC to develop and execute compliant business associate agreements.

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

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

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

- **Qualifications**
  Must be familiar with the practice of medical care within the UEC; 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.

Workforce Training

Purpose

To ensure that the UEC workforce has the training it needs to carry out required job functions.

Policy

The UEC must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.

Procedure

1. New Employees
    a. The Clinic Operations Supervisor will organize and facilitate appropriate training of the new employee by completing the following items.
        i. Assign and complete the New Employee Training Check-sheet to be filed with the employee's employee record.
        ii. Original certificates of completion are to be given to the employee.
        iii. Copies of completed training certificates are to be filed with the Privacy Officer.
        iv. The training is to be completed within a reasonable period of time after the new employee begins working at the Clinic.
        v. The training is to be completed annually and / or with any updates to policies, procedures or laws effecting the areas of training.
        vi. Employee will sign a Data Security Agreement to be filed with the Privacy Officer.
        vii. Employee will sign a Confidentiality Agreement to be filed with the Security Officer.

2. Students and Student Employees
    a. The Clinic Operations Supervisor will organize and facilitate appropriate training of the student or student employee by completing the following items.
        i. Assign and complete the Student Orientation Check-sheet to be filed with the student's or student's employee record
        ii. The training is to be completed prior to the student or student employee's first day on the job. The training is to be completed prior to the student's or new employee's first day on the job.
        iii. The training is to be completed annually and / or with any updates to policies, procedures or laws effecting the areas of training.
        iv. Student or Student Employee will sign a Data Security Agreement to be filed with the Privacy Officer.
        v. Student or Student Employee will sign a Confidentiality Agreement to be filed with the Security Officer.
        vi. The training is to be completed annually and / or with any updates to policies, procedures or laws effecting the areas of training.

3. Annual Student or Employee Training and Refreshers
    a. All UEC will participate in annual HIPAA, Privacy Rule and Data Security trainings as needed. When changes are made to policies and procedures, updates are made by HHA or other governmental agency, training will be provided. Refreshers and reminders will be ongoing.

4. UEC will 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 six years from the date each training session was concluded or last effective date, whichever is later.

SAFEGUARDS

PURPOSE

The purpose of this policy is to provide guidelines for the safeguarding of Protected Health Information ("PHI") in the UEC and to limit unauthorized disclosures of PHI that is contained in a patient's Medical Record, while at the same time ensuring that such PHI is easily accessible to those involved in the treatment of the patient.

POLICY

The policy of UEC is to ensure, to the extent possible, that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other federal or state regulation governing confidentiality and privacy of health information. The following procedure is designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that is, or will be, contained in a patient's Medical Record. At the same time, the UEC recognizes that easy access to all or part of a patient's Medical Record by health care practitioners involved in a patient's care (nurses, attending and consulting physicians, therapists, and others) is essential to ensure the efficient quality delivery of health care.

All staff members are responsible for the security of the active Medical Records within the clinic.

PROCEDURE

The UEC Privacy Officer shall periodically monitor the UEC's compliance regarding its reasonable efforts to safeguard PHI.

Safeguards for Verbal Uses

These procedures shall be followed, if reasonable by the UEC, for any meeting or conversation where PHI is discussed.

Meetings during which PHI is discussed:

1. Specific types of meetings where PHI may be discussed include, but are not limited to:
    a. Compliance Meetings
    b. Clinical meetings
    c. Patient / Client Referral Meeting (Personal Counseling for example)
    d. Bill review meetings
2. Meetings will be conducted in an area that is not easily accessible to unauthorized persons.
3. Meetings will be conducted in a room with a door that closes, if possible.
4. Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.
5. Only staff members who have a "need to know" the information will be present at the meeting.
6. The PHI that is shared or discussed at the meeting will be limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

Telephone conversations:

1. Telephones used for discussing PHI are located in as private an area as possible.
2. Staff members will take reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
    a. Lowering the voice
    b. Requesting that unauthorized persons step away from the telephone area

c. Moving to a telephone in a more private area before continuing the conversation

3. PHI shared over the phone will be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure.

In-Person conversations:

- In examination or other patient care rooms
- With patient in public areas
- With authorized staff in public areas

Reasonable measures will be taken to assure that unauthorized persons do not overhear conversations involving PHI. Such measures may include:

1. Lowering the voice
2. Moving to a private area within the UEC
3. If in a patient room, pulling the privacy curtain, ensuring the door is closed, etc.

Safeguards for Written PHI

All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or individual.

Active Records Within the UEC Clinic:

1. Active Medical Records shall be stored in an area that allows staff providing care to patients to access the records quickly and easily as needed.
2. Authorized staff shall review the Medical Record on their authorized mobile device or in the Records Area.
3. Active Medical Records shall not be left unattended in the UEC anywhere an unauthorized individuals could easily view the records.
4. Only authorized staff shall review the Medical Records. All authorized staff reviewing Medical Records shall do so in accordance with the minimum necessary standards.
5. Medical Records shall be protected from loss, damage and destruction.

Active Financial Office Files:

Active Financial Office Files shall be stored in a secure area that allows authorized staff access as needed.

Thinned Records, Inactive Medical Records:

1. Purged and inactive Medical Records will be filed in a systematic manner in a location that ensures the privacy and security of the information. The Admissions Clerk or a designee shall monitor storage and security of such Medical Records. When records are left unattended, records will be in a locked room, file cabinet or drawer.
2. The Privacy Officer will identify and document those staff members with keys to stored Medical Records. The minimum number of staff necessary to assure that records are secure yet accessible shall have keys allowing access to stored Medical Records. Staff members with keys shall assure that the keys are not accessible to unauthorized individuals.
3. Inactive Medical Records must be signed out if removed from their designated storage area. Only authorized persons shall be allowed to sign out such records.
4. Records must be returned to storage promptly.
5. In the event that the confidentiality or security of PHI stored in an active or inactive Medical Record has been breached, the UEC Privacy Officer shall be notified immediately.

Inactive Business Office Files:

Inactive Business Office Files shall be stored in a systematic manner in a location that ensures privacy and security of the information.

PHI Not a Part of the Designated Record Set:

1. Any documentation of PHI shall be stored in a location that ensures, to the extent possible, that such PHI is accessible only to authorized individuals.

Off - Campus Medical Chart Procedures

The primary purpose in allowing medical charts and related patient information Off- Campus to satellite facilities is in order to provide the treatment necessary at such facilities. Providers and students need access to information from prior records in order to provide treatment in a timely manner. This would include paper charts of prior examinations, as well as anything else needed for a particular day's visit (route slips, consent forms, Notice of Privacy Practices, etc.).

In the continuing effort to safeguard such records, the following practices will be used:

1. The charts and associated documentation for the visit will be sorted and prepared the day before the Off-Campus trip.
2. The official vehicle used will be procured at least one day in advance.
3. A listing of patients will be placed on top of the charts. The list will include:
    a. The patient's name
    b. The name of the person responsible for transporting the charts
    c. The time and date the charts left the main clinic
    d. The time and date the charts returned to the main clinic
    e. The signature and date of the responsible person transporting the charts
4. All the protected health information materials, including the list, will be placed in a locked container.
5. The charts and aforementioned list, will accompany the responsible person to the Off-Campus facility with appropriate annotations on the list. At no time will the charts or list leave the responsible person's security during transport.
6. The same procedure will be used for returning the charts and any new records generated at the Off-Campus facility.
7. Upon return to the main clinic, the time and date of return is noted on the list and the records are secured in the main clinic area.

Office Equipment Safeguards

Computer access:

1. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals.
2. All users of computer equipment must have unique login and passwords.
3. Passwords shall be changed according to University schedules.
4. Posting, sharing and any other disclosure of passwords and/or access codes is **strongly discouraged.**
5. Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment or health care operations.
6. UEC staff members shall log off their workstation when leaving the work area.

7. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.
8. Employee access privileges will be removed promptly following their departure from employment.
9. Employees will immediately report any violations of this Policy to their supervisor, UEC Privacy Officer.

Printers, copiers and fax machines:

1. Printers will be located in areas not easily accessible to unauthorized persons.
2. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment.
3. Documents containing PHI will be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location.

Documents containing PHI that must be disposed of due to error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding

Destruction

Records will be stored, maintained and destroyed according to the University schedule.

Written:

Documentation that is not part of the Medical Record and will not become part of the Medical Record shall be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

Electronic:

Prior to the disposal of any computer equipment, including donation, sale or destruction, the UEC in conjunction with Information Technology Services and / or the equipment vendor must determine if PHI has been stored in this equipment and will delete all PHI prior to the disposal of the equipment.

COMPLAINTS

HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

In order to comply with HIPAA's Privacy Rule, it is the policy of UEC to accept complaints from patients who believe that UEC has not properly respected their privacy, and to thoroughly investigate and resolve them.

1. The Privacy Officer is responsible for accepting all patient complaints about alleged privacy violations. We require all complaints to be in writing. If a complaint comes over the telephone, the Privacy Officer will inform the patient to send it in writing. This can be hard copy or electronic, as the patient wishes. If a patient wishes to remain anonymous, UEC will accommodate that to the extent practical.

2. The Privacy Officer will keep all patient complaints for at least six years. These will be stored, along with information about the investigation and resolution of the complaint, in the office of the Privacy Officer.

3. Upon receiving a patient complaint about privacy, the Privacy Officer will investigate it. The Privacy Officer has discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. Generally, the Privacy Officer will do at least the following in order to investigate a complaint:

a. Talk to the person in the office whom the patient thinks violated the patient's privacy.

b. Review the patient's clinical chart.

c. Talk to other office staff about the patient's concern.

d. Talk to the patient.

e. Review any information or evidence that the patient presents in support of the claim of a violation of privacy.

4. Based upon the results of the investigation, the Privacy Officer will determine if the patient's complaint is substantiated or not. If the complaint is not substantiated, the Privacy Officer will notify the patient in writing. If it is substantiated, the Privacy Officer will determine what steps are necessary to resolve the issue so that it does not recur.

5. In determining what steps are necessary to resolve a substantiated complaint of a violation of privacy, the Privacy Officer will consider at least the following points:

a. What caused the privacy violation?

b. If the violation was caused by a failure to comply with existing policy, the Privacy Officer will report the issue to the Assistant Dean for Clinical Education for action as a human resources disciplinary matter.

c. If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the Privacy Officer will determine how the policy should be changed, or if a policy needs to be developed. If policy revisions or new policies are needed, the Privacy Officer will accomplish that.

d. If a business associate was involved in the violation, what must the business associate do to prevent the violation from recurring. If the business associate cannot cure the breach,

the business associate contract must be terminated. The Privacy Officer will obtain approval from management before any business associate contracts are terminated.

e. If the privacy violation caused harm, what steps are necessary to mitigate that harm? The Privacy Officer will accomplish the steps.

f. If the privacy violation resulted in a breach of PHI, the Privacy Officer will follow the breach notification policies and procedures.

6. Once a resolution of a complaint is determined, the Privacy Officer will take the steps identified as necessary for the resolution.

7. If new policies or procedures are put into place as part of the resolution, the Privacy Officer will conduct mandatory training for UEC workforce regarding them.

8. The Privacy Officer will develop a way to monitor whether the resolution is working to improve UEC privacy protections. If the Privacy Officer discovers continued problems through monitoring, the Privacy Officer will fix the problem.

SAMPLE
COMPLAINT REGARDING USES/DISCLOSURES
OF PROTECTED HEALTH INFORMATION

Tracking Number_____

This form is to be used to file a complaint with the UEC regarding its privacy policies and procedures, and its compliance with those policies and procedures or the federal Privacy Rule.

When this form is complete, please return it to: _____

Patient Information	**Requester's information (if not the patient)**
_____ Name	_____ Name
_____ Address	_____ Relationship to the Customer
_____ Date of Birth _____ Student Number	_____ Source of Legal Authority
_____ Phone Number	_____ Phone Number

Date of incident: _____/or ☐ The practice is ongoing

Time of incident: _____/or ☐ Not applicable

Please describe the practice or incident about which you wish to complain:

_____
_____
_____

Name & title of person(s) involved, if known: _____

Please describe why you believe that this practice or incident was improper:

_____
_____
_____

Please attach any documentation that supports your complaint to this form.

I certify that the information recorded above is true to the best of my knowledge, and that I have a good faith belief that such practice or incident is a violation of federal laws regarding the handling of a patient's health information or of the UEC's privacy policies and procedures.

Signature: _____ Date: _____

RESOLUTION OF COMPLAINT REGARDING USES/DISCLOSURES OF PROTECTED HEALTH INFORMATION

Person investigating the complaint:

Name_____

Title_____

Tracking Number: _____

Date_____

Resolution or Conclusion of investigation:

_____

_____

_____

Comments:

_____

_____

_____

Date and Time Resolution Communicated to Individual:

_____

Approval of Privacy Officer

Name _____ Date_____

Comments/Instructions:

_____

_____

_____

LOG OF INTERNAL COMPLAINTS REGARDING PRIVACY ISSUES

DATE RECEIVED	IDENTITY OF INDIVIDUAL MAKING COMPLAINT (IF KNOWN)	PERSON RECEIVING COMPLAINT	NATURE OF COMPLAINT	STEPS TAKEN TO RESOLVE COMPLAINT	DATE OF RESOLUTION	Method Filed	Tracking Number
Example: 04/30/03	Hotline – anonymous	Pam Peters – privacy officer	Computer screens at nursing station not shielded from visitor view	Computer terminals moved to area at nursing station where they cannot be seen by passerby; monitor screen shields installed	05/02/03		

Discipline

Purpose
To outline sanctions for employee's violations of UEC HIPAA Policies and Procedures.

Policy
Attempting to obtain or use, actually obtaining or using, or assisting others to obtain or use PHI, when unauthorized or improper, will result in counseling and/or disciplinary action up to and including termination.

Procedure.

Definitions and Caveats:

- Depending on the nature of the breach, violations at any level may result in more severe action or termination
- Levels I-III are considered to be without malicious intent; Level IV connotes malicious intent
- At Level IV, individuals may be subject to civil and/or criminal liability
- For any offense, a preliminary investigation will precede assignment of level of violation
- The Privacy Officer shall maintain documentation of all disciplinary actions that UEC has taken against employees for violations of these Policies and Procedures or the Privacy Rules, for a period of six years from the date of the disciplinary action.

Level of Violation	Examples	Minimum Disciplinary/Corrective Action
Level I	• Misdirected faxes, e-mails & mail. • Failing to log-off or close or secure a computer with PHI displayed. • Leaving a copy of PHI in a non-secure area. • Dictating or discussing PHI in a non-secure area (lobby, hallway, cafeteria, and elevator). • Failing to redact or de-identify patient information for operational/business uses. • Leaving detailed PHI on an answering machine. • Improper disposal of PHI. • Transmission of PHI using an unsecured method.	• First offense: verbal counseling • Second offense within one year: written warning. • Third offense within one year: termination. • Notify Privacy Officer of all incidents.
Level II	• Requesting another individual to inappropriately access patient information. • Inappropriate sharing of ID/password with another coworker or encouraging coworker to share ID/password.	• First offense: written warning. • Second offense within one year: termination. • Notify Privacy Officer of all incidents.

	• Failure to secure data on mobile devices through encryption/password.	
Level III	• Releasing or using aggregate patient data without facility approval for research, studies, publications, etc. • Accessing or allowing access to PHI without having a legitimate reason. • Giving an individual access to your electronic signature. • Accessing patient information due to curiosity or concern, such as a family member, friend, neighbor, coworker, famous or "public" person, etc. • Posting PHI to social media.	• Termination. • Notify Privacy Officer of all incidents.
Level IV	• Releasing or using data for personal gain. • Compiling a mailing list to be sold for personal gain or for some personal use. • Disclosure or abusive use of PHI • Tampering with or unauthorized destruction of information.	• Termination. • Violation will be reported to appropriate licensing boards and third party agencies when required. • Notify Privacy Officer of all incidents.

Whistleblowers, Crime Victims and Retaliatory Acts

PURPOSE

To document the UEC policy regarding whistleblowers and crime victims and the prohibition of retaliatory acts against them.

POLICY

The UEC is committed to protecting the rights of members of the workforce who disclose protected health information as victims of a crime or who disclose PHI while acting as whistleblowers. Additionally, the UEC prohibits intimidating or retaliating against whistleblowers.

PROCEDURE

1. Disclosures by Whistleblowers
    A. A member of the UEC workforce or a business associate may disclose PHI, as minimally necessary, to the Privacy officer or other oversight entity, if he/she believes in good faith that UEC, a member of its workforce or a business associate has:
        i. engaged in conduct that is unlawful or otherwise violates professional or clinical standards: or,
        ii. that the care, services, or conditions provided by UEC, a member of its workforce, or a business associate potentially endanger one or more patients, workers, or the public
    B. A member of the UEC workforce or a business associate may disclose protected health information under these circumstances to:
        i. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of UEC
        ii. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining their legal options with regard to the conduct that has resulted in the allegation made by the workforce member or business associate.

2. Disclosures by Members of the UEC Workforce Who are Victims of a Crime
    A. A member of the UEC workforce who is the victim of a criminal act, may disclose PHI to a law enforcement official, when necessary, regarding the suspected perpetrator of the criminal act.
    B. Disclosing PHI under these circumstances does not violate UEC's HIPAA privacy policies regarding the proper use and disclosure of protected health information.
    C. A member of the UEC workforce disclosing PHI under these circumstances may disclose the following types of information regarding the suspected perpetrator of the criminal act:
        1. Name and address;
        2. Date and place of birth;
        3. Social security number;
        4. ABO blood type and rh factor;
        5. Type of injury;
        6. Date and time of treatment;
        7. Date and time of death, if applicable;
        8. Description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

3. Refraining from Intimidating or Retaliatory Acts. The UEC may not intimidate, threaten,

coerce, discriminate against, or take other retaliatory action against any individual:

A. For the exercise by the individual of any action taken by the individual in the filing of a privacy-related complaint.
B. For the filing of a privacy-related complaint with the Secretary of the Department of Health and Human Services;
C. For testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing or
D. For opposing any act or belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of UEC's policies on the use and disclosure of PHI.

4. Reporting Compliance Incidents. Members of the UEC workforce who are aware of a suspected compliance incident, including fraud, abuse, neglect, lapse of professional judgment or privacy violation, are encouraged to report their observations.

5. Reporting Violations
   A. The Privacy Officer has general responsibility for implementing this policy.
   B. Members of the UEC staff who violate this policy will be subject to disciplinary action up to and including termination of employment or contract with UEC.
   C. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or to the Privacy Officer.
   D. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, UEC will make every effort to handle the reported matter confidentially
   E. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with UEC.

Notice of Privacy Practices Policy

In order to comply with HIPAA's Privacy Rule, it is the policy of UEC to:

1. Distribute a Notice of Privacy Practices ("NPP") to every patient at their first appointment, eyewear pickup, or similar encounter.

- The NPP to use is attached to this Policy. Only the Clinic Operations Supervisor has authority to change this NPP.
- The Check-In Staff is responsible to distribute the NPP.
- The Check-In Staff must give the patient a copy of the NPP when the patient arrives for their first visit.
- The Check-In Staff must ask the patient to sign an acknowledgement of receipt (AOR) of the NPP. And put all signed AORs in the designated area.
- If the patient opts not to sign the AOR, The Check-In Staff must make a note of the fact that you asked and that the patient refused. Put this note in the designated area.
- It is not necessary to give a NPP to a patient every time they come in after their initial visit.
    * At every patient encounter, The Check-In Staff must look in the designated area to determine if the patient has previously signed an AOR.
    * If yes, it is not necessary to give that patient another NPP.
    * If no, then it is necessary to distribute a NPP and ask for signature on an AOR.
- If our first encounter with a patient is electronic, our electronic system will automatically send a NPP and ask for a signed AOR.

2. Post a copy of our NPP on our website, our patient portal, and in our waiting room.

3. Keep a stock of copies of the NPP on our Check-In counter so that patients and visitors can take one, if they wish.

4. Whenever we make a material change to our NPP we must make the revised NPP available upon request, have copies available at any delivery site and post the revised NPP in a clear and prominent location, including on the website, if applicable. We will keep a copy of each version of our NPP for six years after the date it ceases to be effective.

5. We will use and disclose protected health information in a manner that is consistent with HIPAA and with our NPP. If we change our NPP, the revised NPP will apply to all protected health information that we have, not just protected health information that we generate or obtain after we have changed the NPP.

FERRIS STATE UNIVERSITY

University Eye Center

NOTICE OF PRIVACY PRACTICES

Effective Date of Notice: April 14, 2003
Revised: September 23, 2013

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

If you have any questions about this Notice, please contact us at: Clinic Operations Supervisor, Ferris State University, Michigan College of Optometry, University Eye Center, 1124 South State Street, Big Rapids, MI 49307, (231) 591-2020.

WE WILL COMPLY WITH THIS NOTICE

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

OUR COMMITMENT TO PROTECT YOUR HEALTH INFORMATION

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

This Notice informs you about the ways we may use and disclose your health information. This Notice also describes your privacy rights, along with the obligations that we have regarding the use and disclosure of your health information. Federal medical privacy law requires us to:

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

HOW WE MAY USE AND DISCLOSE YOUR HEALTH INFORMATION

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

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

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

- **Treatment**. We may use your health information or disclose it to third parties to aid with your medical treatment. We may disclose health information about you to doctors, nurses, pharmacists, technicians, medical students, or other persons who are involved in taking care of you. For example, we may use your health information to set up an appointment for you; test or examine your eyes; prescribe glasses, contact lenses, or eye medications and faxing the prescriptions to be filled; show you low vision aids; refer you to another doctor or clinic for eye care or low vision aids or services; or get copies of your health information from another professional that you may have been before us.

- **Payment**. We may use your health information or disclose it to third parties in order to obtain payment for the services that we provide to you. For example, we may discuss your health information with your insurer to determine whether our health plan will cover the treatment.

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

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

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

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

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

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

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

- **Public Policy Matters**. We may use or disclose your health information in certain limited instances for matters involving the public welfare, such as:

    - for public health risks (e.g., prevention or control of disease, reporting births and deaths, reporting abuse and neglect) or for research purposes when there are sufficient privacy protections in place.

    - to a health oversight agency for activities authorized by law (e.g., audits, investigations, inspections, and licensure necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws)

    - to law enforcement officials (in response to a court order, subpoena, warrant, summons or similar process or to report certain kinds of crimes) and to national security officials under certain limited circumstances

    - to a funeral director, coroner, or medical examiner to permit them to carry out their duties

- to facilitate organ donation and specified research purposes, so long as certain safety measures are in place to protect your privacy

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

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

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

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

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

You have several rights regarding your health information and we will respect your right to exercise them. If you wish to exercise your rights, you must submit a written request on a standard form we will provide to you. You can obtain this form by calling the Clinic Operations Supervisor, Ferris State University, Michigan College of Optometry, University Eye Center, at (231) 591-2020, or by writing to us at Clinic Operations Supervisor, Ferris State University, Michigan College of Optometry, University Eye Center 1124 South State Street, Big Rapids, MI 49307. The form is also available on our website, www.ferris.edu/eyecenter

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

- **Right To Request Amendments**. If you feel that your health information is incorrect or incomplete, you may ask us to correct the information. You must include with your request an explanation of how and why your health information needs to be corrected. We may deny

your request for correction in certain limited circumstances. If we agree to your request for correction, we will take reasonable steps to inform others of the correction.

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

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

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

- **Right To A Paper Copy Of This Notice**. You have the right to receive a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. You may obtain a copy of this Notice on our website, www.ferris.edu/eyecenter or by writing to us at the address listed above.

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

CHANGES TO THIS NOTICE

We have the right to change the terms of this Notice. We also have the right to make these changes apply to health information we already have about you, as well as any we receive or create in the future. We will post a copy of the most current Notice on our website, www.ferris.edu/eyecenter and in our clinic and have a copy available for you to request and take with you. Please look at the top right-hand comer of the Notice to determine the Notice's effective date.

QUESTIONS OR COMPLAINTS

If you have questions about your privacy rights described in this Notice, or if you believe that we may have violated your privacy rights, please contact us at: Clinic Operations Supervisor, Ferris State University, Michigan College of Optometry, University Eye Center, 1124 South State Street, Big Rapids, MI 49307, (231) 591-2020. You may also file a written complaint with us, as well as with the Department of Health and Human Services. We support your right to protect your health information. **We will not penalize you or retaliate against you for filing a complaint.**

University Eye Center
FERRIS STATE UNIVERSITY

AUTHORIZATION FOR RELEASE OF MEDICAL RECORDS

Patient Name: _____ Date of Birth: _____ Address:
City/State/Zip: _____ Telephone: H_____ W

The following individual/organization is authorized to make the disclosure:	**The purpose of the disclosure is:**
Physician/Medical Office: _____ Street/Suite: _____ City/State/Zip: _____ Phone: _____ Fax: _____	☐ Change of Insurance ☐ Continuation of Care ☐ Referral ☐ Other:_____

The type and amount of information to be used or disclosed is as follows:

☐ 2 years back with most recent records
☐ 5 years back with most recent records
☐ Specific information _____

RESTRICTIONS: Only medical records that have originated through this health care facility will be photocopied unless otherwise requested. This authorization is valid only for the release of medical information dated prior to and including the date the patient signed the authorization.

I understand the information in my health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency syndrome (HIV). It may also include information about behavioral or mental health services, and treatment for alcohol and drug abuse.

This information may be disclosed and used by the

following individual or organization:	
Release to: _____ Street/Suite: City/State/Zip: _____ Phone: _____ Fax:	☐ Please mail copies to the address indicated in previous box. ☐ I am planning to pick-up the copies. Please call me when they have been copied.

I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization I must do so in writing and present my written revocation to the health information management department. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. **Unless otherwise revoked, this authorization will expire on the following date, event, or condition: _____.**
If I fail to specify an expiration date, event or condition, this authorization will expire 1 year from the date signed.

I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. I need not sign this form in order to assure treatment. I understand that I may inspect or obtain a copy of the information to be used or disclosed, as provided in CFR 164.524. I understand that any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules. If I have questions about disclosure of my health information, I can contact the authorized individual or organization making disclosure.

I have read the above foregoing Authorization for Release of Information and hereby acknowledge that I am familiar with and fully understand the terms and conditions of this authorization.

_____ _____
(Date) (Signature of Patient/Parent/Guardian or Authorized Representative)

_____ _____ _____
(Witness) Printed name of authorized representative Relationship/Capacity to Patient

_____
Address and telephone number of authorized representative

Authorization to Use and Disclose PHI

Purpose

The purpose of this Policy is to set forth the UEC's process for the use and disclosure of Protected Health Information ("PHI") pursuant to a written authorization.

Policy

In accordance with the HIPAA Privacy Rule, when PHI is to be used or disclosed for purposes other than treatment, payment, or health care operations, the UEC will use and disclose it only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization will be consistent with the terms of such authorization.

Procedure

Exceptions to Authorization Requirements

PHI may be disclosed without an authorization if the disclosure is:

1. Requested by the patient or his personal representative (authorization is never required);
2. For the purpose of treatment;
3. For the purpose of the UEC's payment activities, or the payment activities of the entity receiving the PHI;
4. For the purpose of the UEC's health care operations;
5. In limited circumstances, for the health care operations of another Covered Entity, if the other Covered Entity has or had a relationship with the patient;
6. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the HIPAA Privacy Rule; or
7. Required by other state or federal law.
8. Related to an individual who has been deceased for at least 50 years.

Use or Disclosure Pursuant to an Authorization

a. When the UEC receives a request for disclosure of PHI, the Privacy Officer, or Designee shall determine whether an authorization is required prior to disclosing the PHI.

b. PHI may never be used or disclosed in the absence of a valid written authorization if the use or disclosure is:

    a. Of psychotherapy notes as defined by the HIPAA Privacy Rule;

    b. For the purpose of marketing; or

    c. For the purpose of fundraising.

c. If the use or disclosure requires a written authorization, the Facility shall not use or disclose the PHI unless the request for disclosure is accompanied by a valid authorization.

d. If the request for disclosure is not accompanied by a written authorization, the UEC Privacy Official shall notify the requestor that it is unable to provide the PHI requested. The Privacy Official will supply the requestor with an *Authorization to Use or Disclose PHI* ("*Authorization*") form.

e. If the request for disclosure is accompanied by a written authorization, the Privacy Official will review the authorization to assure that it is valid (see the "Checklist for Valid Authorization" following this Policy).

f. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the Privacy Official will notify the requestor, in writing, of the deficiencies in the authorization. No PHI will be disclosed unless and until a valid authorization is received.

g. If the authorization is valid, the Privacy Official will disclose the requested PHI to the requester. Only the PHI specified in the authorization will be disclosed.

h. Each authorization shall be filed in the patient's Medical Record.

Preparing an Authorization for Use or Disclosure

1. When the UEC is using or disclosing PHI and an authorization is required for the use or disclosure, the UEC will not use or disclose the PHI without a valid written authorization from the patient or the patient's personal representative.

2. The *Authorization* form must be fully completed, signed and dated by the patient or the patient's personal representative before the PHI is used or disclosed.

3. The UEC may not condition the provision of treatment on the receipt of an authorization except in the following limited circumstances:

    a. The provision of research-related treatment; or

    b. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party (i.e., performing an independent medical examination at the request of an insurer or other third party).

4. An authorization may not be combined with any other document unless one of the following exceptions applies:

    a. Authorizations to use or disclose PHI for a research study may be combined with any other type of written permission for the same research study, including a consent to participate in such research;

    b. Authorizations to use or disclose psychotherapy notes may only be combined with another authorization related to psychotherapy notes; or

    c. Authorizations to use or disclose PHI other than psychotherapy notes may be combined, but only if the UEC has not conditioned the provision of treatment or payment upon obtaining the authorization.

Revocation of Authorization

1. The patient may revoke his authorization at any time.

2. The authorization may ONLY be revoked in writing. If the patient or the patient's personal representative informs the UEC that he/she wants to revoke the authorization, the UEC will assist him/her to revoke in writing.

3. Upon receipt of a written revocation, the Privacy Official will write the effective date of the revocation on the *Authorization* form.

4. Upon receipt of a written revocation, the UEC may no longer use or disclose a patient's PHI pursuant to the authorization.

5. Each revocation will be filed in the patient's Medical Record.

Disclosure to Family or Friends

Purpose
In order to comply with HIPAA's Privacy Rule, the UEC will give patients an opportunity to agree or object to providing their PHI to family or friends who are helping with their care.

Policy
UEC will provide a patient the opportunity to authorize or deny the UEC the authority to give certain and relevant PHI to family and / or friends directly involved in the patient's care.

Procedure
1. If it is necessary or appropriate to inform a close family member or friend who is involved in a patient's care about certain protected health information relevant to their involvement, we will give the patient a chance to agree or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:

    a. Get an oral agreement from the patient that the disclosure is acceptable and document in the Medical Record the oral agreement.
    b. Give the patient a chance to object to the disclosure and document this in the Medical Record.
    c. Infer from the circumstances that the patient does not object. For example, we can reasonably infer that the patient does not object if the family member or friend is in the examining room with patient.
    d. Our general practice will be to obtain written permission or an Authorization to Disclose PHI from the patient. However, if the patient is not present or available when the need arises, or in an emergency situation, we will use our best judgment about whether it is in the patient's best interest to disclose the information.

2. If the UEC makes a disclosure to a close family member or friend under the circumstances described in paragraph 1, we will only disclose information that is relevant to the family member or friend's involvement with the patient's care. Examples:

    a. If the patient's spouse, friend, son or daughter will pick up a prescription, we will provide the prescription.
    b. If a spouse, friend, son or daughter will assist a patient with medication, we will provide information about when and how the medication should be administered.

3. If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will instruct the individual to contact the patient to sign an Authorization to Disclose PHI.

4. In the event that the patient is a minor, the Health Center policy on "Treatment of Minors" will be followed.

Disclosure to Personal Representatives

Purpose

To ensure proper release of PHI to authorized patient personal representatives.

Policy

The UEC, with valid authorization, will allow a patient's personal representative to exercise patient rights on behalf of the patient regarding the use and disclosure of PHI and to give any required permission for a use or disclosure of PHI.

Procedure

Identify and validate Personal Representative of a patient.

1. Adult patients and emancipated minors:

    a. Adult patients are those eighteen years of age, or older.

    b. Emancipated minors are people under the age of eighteen who have the legal right to be treated as an adult.

    c. Generally, adults and emancipated minors personally handle all matters about their protected health information. Sometimes, however, they may be unable to do so because of mental incapacity. In this case, specific legally authorized representatives can substitute for the adult or emancipated minor to sign all permissions and exercise all rights regarding protected health information.

2. Unemancipated minors

    a. An unemancipated minor is a person under the age of eighteen.

    b. Generally, unemancipated minors are not able to handle any matters regarding their protected health information because the law presumes them to be incapacitated. The following people can handle signing all permissions and exercise all rights regarding an unemancipated minor's protected health information:

        i. either parent or a parent appointed by the court with documentation
        ii. a court appointment guardian

3. Deceased patients

    a. The following people have the authority to sign permissions and exercise rights regarding the protected health information of deceased patients:
        i. Executor of the Estate
        ii. Next of Kin with Power of Attorney or other authorization

4. In a few instances, we will not work with the personal representatives listed above. This can happen in the following cases:

a. We think that person claiming to be a personal representative has or may have committed domestic violence, abuse, or neglect against the patient, and it is not in the patient's best interest to treat that person as the personal representative.

b. We think that treating such person as the personal representative could endanger a patient, and it is not in the patient's best interest to treat that person as the personal representative.

5. Before we work with someone claiming to be a personal representative, we will verify their authority and consult General Counsel. If we are unsure of a person's authority to sign permissions or exercise rights regarding protected health information, we will not use or disclose that protected health information until any ambiguity is resolved.

De-identification of Protected Health Information

Purpose

To use only de-identified PHI whenever feasible. Health information is not individually identifiable if it does not identify an individual and if the UEC has no reasonable basis to believe it can be used to identify an individual.

Policy

Sections 164.514(b) and(c) of the Privacy Rule contain the implementation specifications that a covered entity must follow to meet the de-identification standard. The Privacy Rule provides two methods by which health information can be designated as de-identified: Expert Determination or Safe Harbor. UEC will use Safe Harbor. Safe Harbor means that 18 types of identifiers will be removed from the PHI and there is no knowledge that any residual information could lead to identification.

Procedure

1.Remove all potential identifiers including obvious ones like name and social security number, and also:

- all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and [t]he initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

- all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

- voice and fax telephone numbers;

- electronic mail addresses;

- medical record numbers, health plan beneficiary numbers, or other health plan account numbers;

- certificate/license numbers;

- vehicle identifiers and serial numbers, including license plate numbers;

- device identifiers and serial numbers;

- Internet Protocol (IP) address numbers and Universal Resource Locators (URLs);

- biometric identifiers, including finger and voice prints;

- full face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code.

2. Statistical De-Identification: A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable applies such principles and determines that the risk is very small that the information could be used to identify the patient. The methods and the results of the analysis must be documented.

3. Re-Identification: The UEC may assign a code that would allow the information to be re-identified by the UEC as long as the code is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient. The UEC must not use or disclose the code or any other means of record identification for any other purpose and must not disclose the mechanism for re-identification.

LIMITED ACCESS

Purpose

To ensure that staff of the UEC have limited access to PHI.

Policy

UEC will restrict access and uses of protected health information based on the specific roles of the members of the workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

Procedure

1. Access to PHI will be determined by position and job duties.
2. Access will be granted based upon Minimum Necessary Standards.
    a. Clinic Operations Supervisor / Privacy Officer
        i. This position is granted full access to PHI.
        ii. This position assigns all other access of workforce to PHI in Electronic Medical Record (EMR) system.
        iii. This position has access to keys of locked files.
        iv. This position has a unique login and password to the EMR system.
    b. Health Care Providers / Students
        i. These positions have full access to Active PHI to provide patient care.
        ii. These positions have limited access to inactive patient records.
        iii. These positions have a unique log in and password to the EMR system.
    c. Technicians
        i. These positions have full access to Active PHI for the provision of patient care and to assist the medical providers.
        ii. These positions have limited access to inactive patient records.
        iii. These positions have a unique log in and password to the EMR system.
    d. Health Admissions Clerk
        i. This position has limited access to EMR PHI in order to help facilitate patient care and schedule appointments.
        ii. This position may have access to a patient's health insurance and financial and demographic information.
        iii. This position has access to locked paper records for the purpose of facilitating current patient care, record destruction and record retrieval for authorized use and disclosure.
    e. PT Adult / Clerk Typist / Student Employee – Front Office
        i. This position has limited access to EMR PHI in order to help facilitate patient care and schedule appointments.
        ii. This position may have access to a patient's health insurance and financial and demographic information.

f. Account Clerk
    i. This position has limited access to PHI for the purpose of billing and managing the patient account.
    ii. This position has a unique log in and password to the EMR system.
g. Medical Records, Billing, Insurance and Coding Specialist
    i. This position has full access to the EMR system in order to facilitate patient care, process billing and medical claims, and to manage the requests and releases for PHI.
    ii. This position has a unique log in and password to the EMR system.
    iii. This position also has full access to the electronic medical claims clearing house database, Navicure.
h. Student Employee – Patient Check-out
    i. These positions have limited access to PHI to facilitate patient check-out.
    ii. These positions have unique login and password to the EMR system.

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, UEC 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. Administrator, doctors, nurses - any and all protected health information, including the entire clinical chart, for treatment payment and health care operations.

    b. Coders/billers and office staff- 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 two locked doors. Only authorized staff will have access to this secure storage. We require that all computers be turned down when the user is away from the workstation. All staff is prohibited from browsing at someone else's workstation or using their computer password. Staff is prohibited from talking about our 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 or Physician 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 or Physician 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.

Use and Disclosure and Requests for Medical Records

Purpose

To ensure that disclosure of Protected Health Information ("PHI") is made consistent with applicable laws, regulations and health information standards, and to ensure that any disclosures of a patient's PHI to a patient's family members, other relatives, close friends or other persons designated by the patient are appropriate.

Policy

Disclosure of PHI will only be allowed with a properly completed and signed authorization except:

- When required or allowed by law (see "Request and Disclosure Table" following this Policy).
- As defined in the *Notice of Privacy Practices*:
  - For continuing care (treatment)
  - To obtain payment for services (payment)
  - For the day-to-day operations of the facility and the care given to the residents (health care operations)

Disclosure of PHI will be centralized through the UEC Privacy Officer. In some instances, the UEC Privacy Officer will need to track information that is disclosed. All disclosures designated as trackable on the "Request and Disclosure Table" must be approved by the Privacy Officer to enable the UEC to provide an accounting of disclosures when requested.

Disclosure of PHI will be carried out in accordance with all applicable legal requirements and in accordance with UEC policy.

Original Medical Records will not be removed from the premises, except when authorized by clinical activities, ordered by subpoena or by other court order.

Procedure

Receiving a Request for Medical Records:

Requests for Medical Records shall be managed by the Privacy Officer, or Designee.

1. Other staff members will not release PHI without approval of the Privacy Official, or Designee.

Responding to Specific Types of Requests:

See the "Request and Disclosure Table" following this Policy for applicable requirements in responding to requests by specific entities/individuals.

1. Media: No PHI shall be released to the news media or commercial organizations without the authorization of the patient or his personal representative.
2. Telephone Requests: Staff members receiving requests for PHI via the telephone will instruct the caller that they cannot verify or deny the patient had been seen until a valid authorization is on file.

Disclosures to Persons Involved with a Patient's Care:

1. The UEC may disclose to a family member, other relative, close friend, or any other person identified by the patient, PHI:

a. That is directly relevant to that person's involvement with the patient's care or payment for care; or
b. Related to the patient's location, general condition, or death

2. Conditions if the Patient is Present**.** If the patient is present for, or otherwise available, prior to a permitted disclosure, then the UEC may use or disclose the PHI only if the UEC:

   a. Obtains the patient's agreement; or

   b. Provides the patient with an opportunity to object to the disclosure, and the patient does not express an objection (this opportunity to object and the patient's response may be done orally).

Requestor	***Authorization Required?***	***Copy Fee Charged?***	***Track on Accounting of Disclosure?***	***Notes:***
Accrediting Agencies (ASCO)	No	No	No	See policy on Business Associates
Attorney for Patient	Yes	Yes	No	See policy on Authorizations
Attorney for Ferris State University	No	No	No	
Contractors/ Business Associates	No, unless their purpose falls outside of TPO	No	No	See policy on Business Associates
For Persons Deceased less than 50 years ❑ Coroner or Medical Examiner, Funeral Directors ❑ Organ Procurement	No	No	Yes	See policy on Accounting of Disclosures
Employer ❑ PHI specific to work related illness or injury, and ❑ Required for employer's compliance with occupational safety and health laws ❑ Health care provided at the request of the employer ❑ Notice is given to the individual that PHI will be disclosed to employer	No, for the purpose listed. Yes for all others.	No	Yes	
Family Members	No for oral disclosures to family members involved in care; Yes for others	Yes	No	See policy on Authorizations

Requestor	*Authorization Required?*	*Copy Fee Charged?*	*Track on Accounting of Disclosure?*	*Notes:*
Entity Subject to the Food and Drug Administration ❑ Adverse events, product defects or biological product deviations ❑ Track products ❑ Enable product recalls, repairs, or replacements ❑ Conduct post marketing surveillance	No	No	Yes	See policy on Accounting of Disclosures
Health Oversight ❑ Government benefits program ❑ Fraud and abuse compliance ❑ Civil rights laws ❑ Trauma/tumor registries ❑ Vital statistics ❑ Reporting of abuse or neglect	No	No	Yes	See policy on Accounting of Disclosures
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No	Part of treatment
Health Care Practitioners and Providers if <u>not</u> Involved in Care or Treatment (i.e., consultants) but conducted for a permitted operational purpose	No	No	No, assuming it is for a permitted operational purpose	Part of operations
Insurance Companies/Third Party Payors Related to Claims Processing	No	No	No	Part of payment
Judicial and Administrative Proceedings ❑ Court order, or warrant ❑ Subpoena	No No - See policy on Responding to a Subpoena	No Yes	Yes Yes	See policy on Accounting of Disclosures

Requestor	*Authorization Required?*	*Copy Fee Charged?*	*Track on Accounting of Disclosure?*	*Notes:*
Law Enforcement ❑ Administrative request ❑ Locating a suspect, fugitive, material witness or missing person ❑ Victims of crime ❑ Crimes on premises ❑ Suspicious deaths ❑ Avert a serious threat to health or safety	No	No	Yes, except for disclosures to correctional institutions.	See policy on Accounting of Disclosures
Public Health Authorities ❑ Surveillance ❑ Investigations ❑ Interventions ❑ Foreign governments collaborating with US public health authorities ❑ Recording births/deaths ❑ Child/elder abuse ❑ Prevent serious harm ❑ Communicable disease	No	No	Yes	See policy on Accounting of Disclosures
Research (w/o Authorization)	No, if IRB or Privacy Board approves the research study and waives authorization.	No	Yes	See policy on Uses and Disclosures for Research and policy on Accounting of Disclosures
Resident/Resident's Personal Representative	No	Yes	No	See policy on Authorizations
Specialized Government Functions ❑ Military and Veterans' activities ❑ Protective services for the President ❑ Foreign military personnel ❑ National security and intelligence activities	No	No	Yes, except for disclosures for national security and intelligence activities.	See policy on Accounting of Disclosures
Workers' Compensation ❑ Comply w/existing laws (see state law)	No	See applicable state law	Yes	See policy on Accounting of Disclosures

Marketing and Fundraising

Purpose

To ensure that all marketing and fundraising communications comply with the HIPAA Privacy Rule's requirements, as well as any applicable state laws or regulations. The goal is for the UEC to safeguard the patient's PHI when engaging in permitted marketing or fundraising activities.

Policy

Marketing communications utilizing PHI require a prior written authorization from the patient with certain defined exceptions.

Fundraising communications that are made specifically for the benefit of the UEC and contain only demographic information and dates of service do not require an authorization as long as the Facility's *Notice of Privacy Practices* describes this limited use of PHI.

Procedure

Marketing

1. The Privacy Rule defines marketing as a communication and/or disclosure of PHI that encourages an individual to use or purchase a product or service, except under the following conditions:
    a. Communications made directly by the UEC to describe a health related product or service it provides.
    b. Communications made for treatment of the individual.
    c. Communications to direct or recommend alternative treatments, therapies, and health care providers or settings of care.
    d. Face to face communications made by the UEC representative to an individual.
    e. Promotional gifts of nominal value (defined in policy; for example, less than $25 each gift not to exceed $100.00 per annum) provided by the UEC.
    f. Communications about government and government-sponsored programs such as communications regarding Medicare or Medicaid eligibility.
    g. Marketing also does not include communications made for the following purposes, unless the UEC or FSU is paid by a third party to do make the communication:
        - Treatment.
        - Case management/care coordination or recommending alternative treatments.
        - To describe a health-related product or service provided by the covered entity including participation in a health care provider network or health plan network; replacement of or enhancements to a health plan; health-related products or services available only to a health plan enrollee that add value to but are not part of a plan of benefits.
2. UEC must obtain a valid, completed *Authorization to Use or Disclose Protected Health Information ("Authorization")* form prior to using or disclosing PHI for purposes that meet the HIPAA definition of marketing and do not qualify for any of the exceptions listed in Item 1 above.
    a. The authorization must conform to the authorization policy.

b. If direct or indirect remuneration to the UEC from a third party is involved, the authorization must state the nature of such third party remuneration.

3. No authorization is required in the following situations:

   a. Communications directed at an entire population (not to a targeted individual) that promote health in a general manner and do not endorse a specific product or service;

   b. PHI is not disclosed in a marketing communication (such as a newspaper advertisement).

4. In the event a planned marketing activity involves payment to the UEC (e.g., cash, referral, gifts, etc.), anti-kickback, inducement, self-referral and general fraud and abuse statutes and regulations may apply. These shall be considered and approved prior to implementation of the marketing activity. The Facility will assure that any marketing activity is in compliance with such laws and regulations.

5. Business Associates and other third parties:

   a. The UEC may engage a marketing firm to conduct permitted marketing activities on the UEC's behalf. Should the marketing activities require the use or disclosure of PHI to the marketing firm, then a Business Associate relationship would exist and a BA Agreement/Addendum would be required. (See the Policy "Business Associates.")

   b. The Facility may not sell or disclose PHI to a third party to help the third party market its own products or services without a signed authorization from the patient. (See Policy "Authorization for Release of Protected Health Information.")

Fundraising

1. When fundraising for its own benefit, the UEC may use or disclose without authorization the following PHI to a Business Associate or to an institutionally related foundation, such as a nonprofit charitable foundation to act on the UEC's behalf:

   a. Demographic information relating to an individual, and

   b. Dates of health care provided to an individual.

2. The Facility's *Notice of Privacy Practices* must include the following information:

   a. The Facility or its agent may contact the patient to raise funds for the UEC, and

   b. The patient may opt out of receiving any fundraising communications.

3. With each fundraising communication made to an individual the UEC must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

4. The UEC will not condition treatment or payment on the individual's choice with respect to the receipt of fund-raising communications.

5. The UEC will not make fund-raising communications to an individual under this paragraph where the individual has elected not to receive such communications.

6. The UEC may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

Sale

Purpose

To ensure that any sale of PHI complies with the HIPAA Privacy Rule's requirements, as well as any applicable state laws or regulations.

Policy

The UEC's general policy is not to sell PHI of its patients. Any sale of PHI would require approval by the Privacy Officer. Before such a sale could occur, the UEC would first have to obtain authorization from each individual whose information was to be sold

Procedure

Definition. "Sale of PHI" means any disclosure of PHI where the UEC 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 UEC 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 UEC 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 UEC and related due diligence.
- To a business associate for activities that the business associate undertakes on behalf of the UEC, if the only remuneration is provided by the UEC 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 UEC 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.

RESEARCH

PURPOSE

This policy dictates the circumstances under which the UEC can use PHI for research purposes and share information with other individuals or organizations for research purposes.

OBJECTIVE

Clinical research activities may occur in the UEC involving patients.

DEFINITIONS

Clinical Study – a closely supervised investigative process which aims to determine or confirm how a product or technique works in human patients/subjects, also called Clinical Trial.

Human Subject – a living subject participating in research about whom directly or indirectly identifiable health information or data are obtained or created.

Indirectly Identifiable – data that do not include personal identifiers, but link the identifying information to the data through use of a code.

Individually Identifiable Health Information – a subset of health information that identifies the individual or can reasonably be used to identify the individual.

Informed Consent – process of educating subjects about the study that begins at the initial contact between the investigators and the subject and continues throughout the duration of participation; see the section below on Informed Consent.

Institutional Review Board (IRB) – mandated method of peer review to protect human subjects.

Investigators – individuals conducting human subject research, including, but not limited to physicians, students, and administrative staff, also called Researchers.

Legally Effective Informed Consent – when informed consent is obtained from both the subject or the subject's legally authorized representative and it is documented in a manner that is consistent with the Department of Health and Human Services protection of human subjects regulations and applicable laws of the jurisdiction in which the research is conducted.

Preceptor – faculty or staff member responsible for upholding rules and protocols during research activities

Privacy – an individual's interest in limiting who has access to personal health care information; definition for purposes of the HIPAA Privacy Rule.

Protocol – a carefully designed and detailed plan that is developed and then reviewed by a committee of experienced people.

Research – any systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Waiver of Authorization – under limited circumstances, a waiver of the requirement for authorization for use or disclosure of private health information may be obtained from the IRB by the researcher. This can be approved only if specific criteria have been met.

PATIENT RIGHTS RELATED TO THIS POLICY

HIPAA privacy regulations require an IRB to protect the privacy rights of research subjects in specific ways. For instance, IRBs may review HIPAA-required authorization and waiver of authorizations for research use of identifiable health information.

Patients have the right to privacy of care. Students in clinical training may observe the delivery of health care to research subjects and perform certain testing or take measurements concerning a research subject's eye health. If the research subject objects to having a student present, no students except those involved in direct care will be present during any procedure, examination, or consultation.

Patients also have the right to talk privately with their health care providers. They also have the right to keep their personal health information protected. The University Eye Center's Security Policy provides a complete list of safeguards the UEC uses to protect PHI.

Research subjects have the right to informed consent, including the right to withdraw from the study at any time.

For a complete list of patient rights, please see the University Eye Center's Patient Bill of Rights.

RESEARCH

In addition to uses and disclosures that are otherwise permitted under these policies and procedures we may disclose subject to these research policies.

Research, as stated above, is any systematic investigation designed to develop or contribute to generalizable knowledge. The HIPAA Privacy Rule permits a covered entity to use and disclose PHI for research purposes, without an individual's authorization, provided the covered entity obtains any of the following:

(1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of PHI about them for research purposes has been approved by an IRB or Privacy Board.

(2) representations from the researcher that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any PHI from the covered entity, and that PHI for which access is sought is necessary for the research.

(3) representations from the researcher that the use or disclosure sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals

about whom information is sought. A covered entity also may use or disclose, without an individuals' authorization, a limited data set of PHI for research purposes.

(4) Limited Data Set. This may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement with UEC promising specified safeguards for the PHI within the limited data set.

UEC may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make. For further details on permitted uses and disclosures, please reference the most updated version of the Ferris State University Eye Center Clinic Manual.

PATIENT ACCESS

A patient's right to access their PHI created or obtained by the UEC in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in the research that includes treatment, and the UEC has informed the individual that the right of access will be reinstated upon completion of the research. Additionally, product information that is being used during the study is confidential with the manufacturer and cannot be disclosed to the individual as it may create bias affecting the results of the study.

ACCOUNTING FOR DISCLOSURES

If a patient requests an accounting of disclosures for a time period in which the UEC has made disclosures of PHI for a particular research purpose for 50 or more individuals, the accounting may, with respect to those disclosures include:

(1) The name of the protocol or other research activity;

(2) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(3) A brief description of the type of PHI disclosed;

(4) The date or period of time during which the disclosures occurred, or may have occurred, including the date of the last disclosure during the accounting period;

(5) The name, address, and telephone number of the entity that sponsored the research and of the research to whom the information was disclosed; and

(6) A statement that the PHI of the patient may or may not have been disclosed for a particular protocol or other research activity.

If it is reasonably likely that the PHI of the patient was disclosed for the research protocol or activity, the UEC must, at the request of the patient, assist in contacting the entity that sponsored the research and the researcher.

RULES FOR RESEARCHERS

The researchers, including but not limited to faculty, staff, and students, will adopt at least the following practices:

- No spoken conversations about or to a participant within hearing distance of anyone not involved in that participant's care. Discretion will be used by other faculty, staff, and students not directly involved in the research but who are affiliated with UEC and/or UEC. All discussions about identifiable PHI shall only occur in the designated research areas.

- All participant information and data must be secured and stored properly when a research area is vacated.
- All participant and research correspondence, such as data analysis and summary reports, must be done in the confines of UEC and UEC, unless specifically approved by the preceptor of the research.
- PHI that will be used for research or generated on printed reports must be removed from the data set as defined by the limited data set above. This can include printing the research and exam elements, then removing the PHI.
- The use of portable memory devices is prohibited, unless specifically approved by the preceptor of the research, to reduce the chance of ePHI loss and protect our systems from malicious software.
- Each researcher is assigned a unique password only known to the user. This password is not to be shared with anyone. Only the designated system administrator has rights to reset any given password.

CONTACT PERSON

If there are any questions regarding this policy, please contact the Clinical Operations Supervisor, by mail, phone, or fax, at:

University Eye Center
1124 S State Street
Big Rapids, MI 49307
Phone: (231)591-2020
Fax: (231)591-3551

Business Associate Agreements

Purpose

The purpose of this Policy is to provide a process for establishing a written agreement with each of the UEC's Business Associates ("BA") as required by the HIPAA Privacy Rule.

Policy

The UEC contracts with various outside entities and organizations to perform functions or provide services on behalf of the UEC that may involve the disclosure of Protected Health Information ("PHI") to the outside entity. These outside entities are the UEC's Business Associates. The policy of this UEC is to obtain written assurances from BAs that they will appropriately safeguard any PHI they create or receive on the UEC's behalf. Such written assurances will be in place before the UEC discloses PHI to the Business Associate.

Procedure

1. The Assistant Dean for Clinical Education will forward contracts to be reviewed by General Counsel for contract review, revision and approval to assure that contract is in compliance with state and federal law and policies of the University.
2. For each contract, determine whether a Business Associate Agreement is necessary. Common examples of BAs are:
    a. Accredidation agency
    b. The UEC's EMR vendor.

    Note*:** Business Associate language is ***not required when the BA is a health care provider and all disclosures to the BA concern the treatment of a patient.
3. If a BA Agreement is necessary and the third party provides its own BA Agreement, review the Agreement to assure it meets all requirements of the Privacy Rule.
4. If a BA Agreement is necessary, and the third party does not provide the Agreement, submit UEC's template BA Agreement for approval by the third party.
5. If the BA refuses to sign the BA Agreement, the HIPAA Privacy Rule prohibits the UEC from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of the UEC, the UEC shall not contract with the BA.
6. The original signed contract and contract addendum containing BA language shall be maintained by the UEC and University Purchasing.
7. Violations of BA Requirements - If UEC staff learns of a breach or violation of a BA requirement by a BA, such breach or violation shall be reported to the Privacy Officer, his designee, or to the Compliance Department. The Privacy Officer or Compliance Designee will assist the UEC in determining whether reasonable steps can be taken to cure the breach. If the UEC's reasonable steps to cure the BA's violations are unsuccessful, the UEC may:
    a. Terminate the contract or arrangement; or
    b. If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services.

Notice of Termination of a Contract with a BA - The UEC shall notify the Assistant Dean for Clinical Education, his designee or the Legal Department when issuing or receiving a notice of contract termination involving a BA. The Legal Department will assist with contacting the BA regarding the BA's obligations to return or destroy all PHI or, if return or destruction is not feasible, to extend the protections of the BA requirements to the PHI and to limit further uses and disclosures to those purposes that make the return or destruction of the PHI.

The Assistant Dean for Clinical Education shall maintain copies of all contracts with business associates for a period of six years from the date the contract was last in effect.

Validation of Authorization to Disclose PHI

Purpose

To ensure that Protected Health Information (PHI) is disclosed only to appropriate persons in accordance with the requirements of the HIPAA Privacy Rule.

Policy

It is the policy of UEC to verify the identity and the authority of a person making a request for the disclosure of PHI, if the identity or authority of such person is not known to UEC. Further, UEC will obtain from the person seeking disclosure of PHI such documentation, statement or representation, as may be required by the HIPAA Privacy Rule, prior to a disclosure.

Procedure

1. In general, the UEC may rely on required documentation, statements or representations that, on their face, meet the verification requirements, if the reliance is reasonable under the circumstances. If there are concerns as to the requirements, contact the General Counsel.
2. Administrative Requests, Subpoena and Investigative Demand: Verification is sufficient and the UEC will disclose the requested PHI if the administrative document itself or a separate written statement recites:
    a. The information sought is relevant to a lawful inquiry.
    b. The disclosure complies with the minimum necessary standard or is specifically exempt from the minimum necessary standard.
    c. De-identified information could not be used.
    d. If not accompanied by an order of a court or administrative tribunal, there must be an appropriate protective order in place and, when medical records are involved, documentation that the patient has waived his or her physician-patient privilege.

    Check state laws for any additional restrictions on the right to use or disclose PHI; in a Michigan court case, medical records are subject to a privilege; if the UEC received a subpoena, the UEC 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
3. Requests by a Public Official
    a. It is sufficient verification of the *identity* of the requesting person to rely on any of the following, if reasonable under the circumstances:
        i. A badge or other credential
        ii. A request on government letterhead.
        iii. If the person making the request is acting on behalf of a public official, a written statement on government letterhead that the person is acting on behalf of a public official. If other authority is presented, contact General Counsel for guidance before disclosure.
    b. It is sufficient verification of the *authority* of the requesting person to rely on any of the following, if reasonable under the circumstances:
        i. A written statement of the authority under which the information is requested, for example, a copy of the law or regulation. Rarely, a written statement is impractical, and then an oral statement is sufficient.

ii. Verification of authority is presumed if the request is made pursuant to a warrant, subpoena, order or other process issued by a grand jury, court or judge or administrative tribunal.

4. If the disclosure is sought by persons involved in the patient's care, and it is relevant to the requesting party's involvement in the care, the UEC may rely on reasonable professional judgment in verifying the identity and authority of the person seeking disclosure. If the individual is deceased, UEC may disclose to a family member, or other persons involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

5. Verification requirements are met if the UEC, in good faith, makes a disclosure of PHI:

   a. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public, or

   b. To law enforcement authorities (i) to identify or apprehend an individual; (iii) about an individual who has died; (ii) for identification and location purposes; (iv) about an individual who is, or is suspected of being, a victim of a crime; or (v) about an individual relating to a crime on the premises.

SAMPLE CHECKLIST FOR VALID AUTHORIZATION

When you receive a request for release of Medical Records containing PHI from any entity other than the patient or the patient's personal representative, and the disclosure is not for purposes of treatment, payment or health care operations or another disclosure required or permitted by the HIPAA Privacy Rule, you may not release those records unless the requestor has provided a valid authorization. Use this checklist to assure that the authorization is valid. **If any one element is missing, the Privacy Rule prohibits you from disclosing the information.** You should contact the requestor and explain why you cannot disclose the information.

_____The authorization must be written in plain language.

All of the following elements must be included in the authorization:

_____A specific and meaningful description of the information to be disclosed.

_____The name or other specific identification of the person (or organization or class of persons) authorized to make the requested disclosure.

_____The name or other specific identification of the person (or organization or class of persons) to whom the information will be disclosed.

_____The purpose of the requested disclosure. (If the patient initiates the authorization, the statement "at the request of the patient" is a sufficient description of the purpose).

_____An expiration date or an expiration event that relates to the patient or the purpose of the disclosure.

_____Signature of the patient or personal representative and date.

_____If signed by personal representative, a description of the representative's authority to act for the patient.

Required Statements:

_____A statement that information disclosed pursuant to the authorization may be subject to redisclosure and may no longer be protected by the Privacy Rule.

_____A statement of the patient's right to revoke the authorization in writing and either,

_____A reference to the revocation right and procedures described in the Notice of Privacy Practices;

OR

_____A statement about the exceptions to the right to revoke and a description of how the patient may revoke.

_____One of the following statements, or a substantially similar statement:

- If the Covered Entity is not permitted to condition treatment or payment on the provision of an authorization: I understand that the UEC will not condition the provision of treatment or payment on the provision of this authorization.

OR

- If the Covered Entity is permitted to condition the provision of research-related treatment on the provision of an authorization: I understand that the UEC will not provide research-related treatment to me unless I provide this authorization.

OR

- If the Covered Entity is permitted to condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization: I understand that the UEC will not provide health care that is solely for the purpose of creating PHI for disclosure to *a third party* to me unless I provide this authorization.
-

Defective Authorizations

If an authorization has any one of the following defects, it is invalid and any use or disclosure made pursuant to the authorization will be in violation of the Privacy Rule:

_____The authorization has expired.

_____One of the required elements or statements is missing.

_____The UEC has knowledge that the authorization has been revoked.

_____The authorization violates the regulations governing conditioning treatment or payment upon signing the authorization, or combining authorizations.

_____The UEC has knowledge that information in the authorization is false.

Mitigation of Inadvertent Disclosure

Purpose

To ensure proper mitigation of harm in the event of inadvertent disclosure of PHI occurs by the UEC or one of its Business Associates.

Policy

It is the policy of UEC to mitigate known harm from an inadvertent disclosure of PHI when it is practical to do so.

Procedure

1. Whenever we learn of harm caused by an improper disclosure of our protected health information, we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates.

2. The Privacy Officer will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps include:

    a. 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. The Privacy Officer may consult as necessary with legal counsel.

    b. Document the known details of the unauthorized use or disclosure for purposes of responding to requests for an accounting.

    c. Evaluate current policies and procedures to determine whether modifications are appropriate.

    d. Retrieving PHI that was inadvertently disclosed.

    e. Monetary reparation will not be considered.

    f. If a business associate has made the improper disclosure, we will require the business associate to cure the problem to our satisfaction, or terminate the relationship with the business associate.

    g. The Privacy Officer will determine whether UEC will need to follow the Breach Notification Procedures, below.

Risk Assessment and Management

Purpose
To take security measures to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI (ePHI).

Policy
A periodic risk analysis of the UEC ePHI shall be conducted by the Privacy Officer and/or Security Officer or his/her designee. This risk analysis shall occur at least yearly, and shall be a comprehensive and thorough review of the use, maintenance, and disposal of UEC ePHI.

Procedure
On a regular basis (or whenever environmental or an operational changes occur that significantly impact the confidentiality, integrity or availability of specific information systems that contain ePHI), UEC will conduct the risk assessment using the following steps:

Conduct an Inventory.: Inventory UEC information systems containing ePHI and the security measures protecting those systems.

Identify Threats: Identify the potential threats to the information systems containing ePHI. Such threats may be natural, human or environmental.

Identify Vulnerabilities: Identify the vulnerabilities to the information systems containing ePHI.

Security Control Analysis: Analyze the security measures that have been implemented to protect the information systems (including both preventive and detective controls).

Determine the Likelihood that a Risk Will Be Exploited: Assign a risk rating indicating the probability that a vulnerability will be exploited by a particular threat, taking into account (1) threat motivation and capability, (2) the type of vulnerability, and (3) the existence and effectiveness of current security controls.

Determine the Likely Impact if a Vulnerability Is Exploited: Determine the impact to confidentiality, integrity or availability that would result if a threat were to successfully exploit a vulnerability on a UEC system containing ePHI.

Identify the Level of Risk for each Vulnerability and Associated Possible Threat: Based on the above analysis, assign a risk level to each vulnerability and associated threat.

Prioritize Risk: In consultation with the relevant individuals, prioritize the risks identified in the risk analysis on a scale from high to low based on the potential impact to information systems containing ePHI and the probability of occurrence.

Evaluate Options to Manage Risks: For those risks determined as significant enough to require further evaluation, identify appropriate security methods to address and manage the risk to UEC information systems.

Perform a Cost-Benefit Analysis: Identify the costs and benefits of implementing or not implementing specific risk management methods.

Select a Risk Management Method: Recommend to the appropriate individuals the most appropriate, reasonable and cost-effective option for managing the identified risks to the information systems containing ePHI. The Security Officer will determine the appropriate risk management method.

Implement the Risk Management Method. Implement the selected risk management methods according to a schedule developed with the Security Officer.

Evaluate the Effectiveness of the Risk Management Method. Establish a schedule to review and evaluate the effectiveness of the implemented risk management methods, and consider revising the method if necessary.

Documentation and Record Retention

Purpose

To create a policy stating that the UEC complies with HIPAA by documenting and retaining compliance records for the later of (i) at least six (6) years from the date of its creation, or (ii) at least six (6) years from the date the document ceased to be effective. Upon expiration of the aforementioned timeline UEC will comply with destruction according to University Record Destruction Policy.

Policy

The UEC and Privacy Officer will document and retain documentation on the following:

1. HIPAA Policies and Procedures
2. Notice of Privacy Practices
3. Disclosures of PHI for Requests for an Accounting
4. Uses and Disclosures that Must Be Documented
5. Uses and Disclosures that Need Not be Documented
6. Authorizations and Individual Rights
7. Training
8. Complaints
9. Disciplinary Action
10. Mitigation Efforts and any risk analysis performed
11. Business Associate Agreements
12. Risk assessments

Procedure

The Privacy Officer will follow the attached policies associated with the above. Except as provided below, each policy requiring documentation provides procedures for that documentation. The Privacy officer will store all documentation in a designated cabinet for all HIPAA compliance activities.

Documenting Authorizations and Individual Rights. The Privacy Officer will maintain under lock and key for a period of six 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 and related communications provided in response to the requests
- 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 and all documents relating to the response to each
- each request to amend PHI and all documents relating to the disposition of each; if the UEC elects to amend the PHI, the amendment must be maintained with the record for as long as the record is maintained; if the UEC 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 all 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 UEC for documents maintained by the UEC. 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.

Patient Access to Their PHI

Purpose

To define *a* patient's right to access their PHI / medical records.

Policy

Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's designated record set. The "designated record set" is that group of records maintained by or for the UEC that is used, in whole or part, to make decisions about patients, or that is a provider's medical and billing records about patients or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, the UEC may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion. The UEC may impose reasonable, cost-based fees for the cost of copying and postage.

Procedure

Request to View Medical Records:

1. Refer the patient or personal representative to the UEC designated Medical Records, Billing, Insurance and Coding Specialist or Health Admissions Clerk.
2. Confirm the requestor has the legal authority to view the record by verifying identity.
3. Set up a meeting within 24 hours as required by law. If the requestor cannot accommodate a meeting within the 24 hour time frame, the review should be set up at a mutually agreed upon time.
4. Assure a staff member is in attendance at all times during the meeting, to
    a. Answer questions,
    b. Assure the record is not altered in any way, and
    c. Assure documents are not removed/destroyed.
5. Allow the patient to review and read the record without intervention from the staff member present.
6. Preferred procedure is to complete an *Access to Protected Health Information* form.
7. If the request involves records used for research purposes, please see the research policy in these policies and procedures.

Request for a Copy of Medical Records:

- Refer the patient or legal representative to the UEC Medical Records, Billing, Insurance and Coding Specialist or Health Admissions Clerk.

- Confirm the requestor has the legal authority to request a copy of the record by verifying identity.
- Although HIPAA does not require the access request to be in writing, the preferred procedure is to complete an *Access to Protected Health Information* form.
- Disclose the UEC's charge for copying to the patient.
- Make reasonable efforts to provide the patient with the copies within two working days but no later than 30 days from the date of the request.

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 to the individual:
    - the basis for the denial. UEC is not required to grant access, and is not required to review its denial, in the following circumstances:
        - information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
        - certain research activities, as further described in the research policies and procedures above;
        - the PHI is contained in records that are subject to the Privacy Act of 1974, if the denial of access under the Privacy Act would meet the requirements of law; or
        - if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
    - if applicable, a statement of the individual's right to have the decision to deny access reviewed
        - UEC is not required to grant access, but must give the individual a right to have the denial reviewed in the following circumstances:
            - 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 such other person; or
            - The request for access is made by the individuals' personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

        - 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 a complaint form for the individual to 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 UEC will designate who will serve as the reviewing official
            - the denial letter must be promptly sent to the individual to notify him or her of the reviewing official's determination
            - the UEC must take any other action required by the reviewing official
        - a description of how the individual may complain to the UEC 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

- 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 or in person)
    - if the individual has requested the information 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 a readable hard copy form or in such other form in which the individual agrees to receive it
    - if the PHI is in coded form, an accurate translation in plain English must be provided
- *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 UEC 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 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
- *Fees.* The UEC may charge the following fees for access to the records
    - the UEC may not charge for retrieving or handling the information
    - if photocopies are requested
        - the UEC may charge for the costs of supplies used in making the copies, including the cost of the paper
        - UEC may charge for the time an employee spent making the copies at the employee's hourly rate; if the employee is a salaried employee, a pro rata hourly rate will be calculated to determine the charge
    - the information is provided on a computer disk or other portable electronic media, the cost of the media may be charged
    - if the request is to have the records sent by mail or other type of delivery service (such as UPS, Federal Express, etc.), the actual cost of the postage or delivery service requested may be charged
    - if the request is for a summary or explanation of the individual's records, the UEC may charge for the time an employee spent preparing the summary or explanation at the employee's hourly rate; if the employee is a salaried employee, a pro rata hourly rate will be calculated to determine the charge
- if the disclosure is made to the parent of a minor or a personal representative, retain documentation of the disclosure as required
- If the UEC maintains the information in an electronic form, the UEC must be able to provide the information in an electronic form to an individual. The UEC 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 UEC cannot provide the information in the requested format, it will offer to produce the information in the formats that are available. If the UEC and the individual cannot agree on an electronic format, the UEC may produce the records in paper form.

FERRIS STATE UNIVERSITY
University Eye Center

REQUEST TO INSPECT AND COPY

Part I: To Be Completed By Health Plan Participant, Covered Spouse or Covered Dependent

1. Please complete the following:

Name: _____

Address: _____

Phone number: _____ Date: _____

Cell Phone: _____

Email address: _____

Date of birth: _____

Social Security Number: _____ _____

2. This request concerns:

___ My health information.

___ The health information of my minor child who is covered by the Health Plan.

Child's name: _____ Child's SSN: _____ Child's date of birth: _____

___ The health information of an individual who is covered by the Health Plan and for whom I am the legal guardian.

___ Copies of documents establishing my legal authority are attached.

___ Copies of documents establishing my legal authority are already on file with the Health Plan

Individual's name: _____ Individual's SSN: _____ Individual's date of birth: _____

3. I would like access to the protected health information in the following manner:

____ I would like to personally review the protected health information records at a mutually convenient date, time and place.

____ I would like to obtain a copy of the protected health information records. (There may be a charge for this service—see below.)

___ I would like the University Eye Center ("UEC") to prepare a summary of the personal health information records. (There may be a charge for this service—see below.)

UEC will normally provide the information within 30 days of this request, if the UEC is unable to provide the information to you in 30 days the UEC will send you a written notification explaining the reasons for the delay and the date by which the information will be available, which will be no longer than 30 days from the original deadline for providing the information.

4. Please provide the information in the following format:

___ I would like to access the records in the same format in which they are maintained.

___ I would like to access paper copies of the records.

___ I would like to access electronic versions of the records, if the documents can be readily produced in an electronic version. For those records not in electronic format, I would like to access a paper copy.

5. Please provide the information to me in the following manner:

___ I will personally pick up or come review the records once you notify me that the records are ready.

___ Please send the information to me by:

___ U.S. postal service, at the address I have listed above.

___ inter-office delivery, to _____.

___ e-mail (if available), at the e-mail address noted above.

___ Other: _____.

6. Fees:

If you are requesting a copy of your protected health information records, the UEC may charge a fee for the actual costs of copying, including the costs of the supplies, whether paper or electronic, and for the labor of making the copies. The UEC may also charge for the actual cost of delivering the documents to you if you have elected to have them sent by U.S. mail or some other service that charges the UEC a fee. If the number of copies is small, the UEC may elect not to charge for the copies. If there will be a charge, someone from the UEC will contact you to provide you with an estimate of the charge, and you can then decide whether you still want a copy of the documents.

If you are requesting a summary of your protected health information, the UEC may charge a fee for the time spent preparing the summary and the costs of delivering the summary to you, if you have elected to have it sent by mail or delivered by some other service. If there will be a charge, someone from the UEC will contact you to provide you with an estimate of the charge, and you can decide whether you still want a summary prepared.

7. Signature of individual:

I hereby warrant that I have truthfully represented my identity and that I am authorized to receive the information that I have requested. I understand that if I have misrepresented my identity or my authority, that the UEC may seek whatever criminal and civil relief is available.

_____ _____

Signature of individual Date

8. Submit this form to the Privacy Officer (MCO-101F).

Part II: To Be Completed By the Privacy Officer.

Received by: _____

Date received: _____

Extension requested: ☐ Yes ☐ No

Reason for extension: _____

Date extension notice sent (attached): _____

Date granted (attached): _____

If granted, date information sent or presented: _____

Date denied (attached): _____

Reason for denial:
☐ PHI not created by UEC
☐ Not permitted by federal law (i.e., Privacy Act, psychotherapy notes)
☐ PHI not a part of employee's designated record set
☐ Other:

_____

_____

Review available: ☐ Yes ☐ No

Review requested: ☐ Yes ☐ No

Reviewer: _____

Date of decision (attached): _____

Decision: _____

Comments: _____

_____

_____

_____

Federal law requires the retention of this document and all documents concerning this matter for a period of six years, beginning on the date of the final disposition of this request.

FERRIS STATE UNIVERSITY
University Eye Center

[Patient address info]

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. Ordinarily, we would be able to respond to your request within 30days, but due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by [insert farthest date].

We look forward to working with you in the future.

[signature block]

FERRIS STATE UNIVERSITY
University Eye Center

[Patient address info]

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. We are pleased to be able to grant this request.

If you want to inspect your information or make copies of it yourself, you may do so at our office during our normal business hours. Please let us know what date and time you would like to come. We will do our best to accommodate your requested date and time.

If you would like us to make a copy of your information for you, we are happy to do so. However, we will charge you a reasonable, cost-based fee for the labor in copying the PHI, whether in paper or electronic form. Additionally, we may charge you for the supplies for creating the paper copy or electronic media if you request it on portable media as well as postage. We require payment of these charges in advance, before we start making copies. If you want us to mail the copies to you, we are again happy to do so, but you must pay us the cost of postage. The postage cost to mail the information that you requested is the prevailing registered mail first class rate.

If you prefer, we can summarize our information and give that to you instead of having you inspect or copy all of the information. If you want to do this, we will charge a reasonable, cost-based fee for labor per summary, and we require payment of this amount before we start making the summary.

You requested the information in [insert form or format requested]. We [can/cannot] accommodate that form or format. [Because we cannot accommodate that form or format, we will provide the information to you in hard copy, unless we can agree upon some other format that we can accommodate.]

Thank you again for your request. We look forward to working with you in the future. [signature block]

FERRIS STATE UNIVERSITY
University Eye Center

[patient address info]

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. Unfortunately, we are unable to permit you to inspect or copy this information.

The reason for this denial is:

[specify one or more permitted reason(s).]

You are entitled to one review of our decision. If you want to request a review, send a written request to the Assistant Dean for Clinical Education at the address shown in our letterhead. The Assistant Dean for Clinical Education will look at the information that you want to inspect or copy, and decide if our decision is correct. If it is, you will not be able to inspect or copy the information. If the Assistant Dean for Clinical Education concludes that we were wrong in denying you access to the information, you will be able to inspect or copy it, and we will be back in contact with you.

You always have the option to complain to us or to the U.S. Department of Health and Human Services – Office for Civil Rights if you think that we have not properly respected your privacy. If you want to complain to us, write or call the Clinic Operations Supervisor at the address or phone number in our letterhead.

Thank you again for your request. We look forward to working with you in the future. [signature block]

Patient Request to Amend PHI

Purpose

This Policy is to provide a process for responding to a patient's request for an amendment to Protected Health Information ("PHI").

Policy

A patient has the right to request that the UEC amend his PHI maintained in the Designated Record Set for as long as the PHI is maintained. The policy of this UEC is to respond to a patient's request for amendment of PHI in accordance with the HIPAA Privacy Rule. This policy contains the procedures for approving an amendment, denying an amendment and making an amendment at the request of another covered entity.

Procedure

1. The patient will be notified of the right to amend his PHI in the *Notice of Privacy Practices.*
2. The UEC Privacy Officer will process all requests for amendment.
3. Upon receiving an inquiry from a patient regarding the right to amend his/her PHI, the Privacy Officer will provide the patient with a copy of an *Amendment of Protected Health Information* ("*Amendment of PHI*") form. A request for amendment will not be evaluated until the request form is completed and signed by the patient or personal representative.

Evaluating and Responding to the Request for Amendment

1. The Privacy Officer will date stamp or write the date received and initial the *Amendment of PHI* form.
2. The Privacy Officer will make a determination to accept or deny the amendment after consultation with the appropriate staff, if needed.
3. The Privacy Officer shall act on the request for amendment no later than 60 days after receipt of the request.
    a. If the amendment is accepted, UEC staff shall make the amendment and inform the patient within 60 days of the written request.
    b. If the amendment is denied, the UEC shall notify the patient in writing of the denial within 60 days of the written request.
4. If the UEC is unable to act on the request for amendment within 60 days of receipt of the request, it may have one extension of no more than 30 days. The Privacy Officer will notify the patient in writing of the extension, the reason for the extension and the date by which action will be taken.

Denial of Request for Amendment

1. The UEC may deny the request for amendment in whole or in part if:
    a. The PHI was not created by the UEC.
    b. The PHI is not part of the Designated Record Set

c. The PHI would not be available for inspection under the HIPAA Privacy Rule.

d. The PHI that is subject to the request is accurate and complete.

4. If the Privacy Officer, in consultation with the appropriate staff, determines that the request for amendment is denied in whole or in part, the Privacy Officer will provide the patient with a timely amendment denial letter. The denial shall be written in plain language and shall contain:

   a. The basis for the denial;

   b. A statement that the patient has a right to submit a written statement disagreeing with the denial and an explanation of how the patient may file such statement;

   c. A statement that, if the patient does not submit a statement of disagreement, the patient may request that the UEC include the patient's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment;

2. A description of how the patient may file a complaint with the UEC or to the Secretary of the U.S. Department of Health and Human Services. The description must include the name or title and telephone number of the contact person for complaints.

3. The patient may submit a written statement of disagreement.

4. If the patient submits a written statement of disagreement, the UEC may prepare a written rebuttal to the statement. The UEC shall provide a copy of the written rebuttal to the patient who submitted the statement.

5. The following documentation must be appended (or otherwise linked) to the PHI that is the subject of the disputed amendment:

   a. The patient's *Amendment of PHI* form;

   b. The UEC's amendment denial letter;

   c. The patient's statement of disagreement, if any; and

   d. The UEC's written rebuttal, if any.

Future Disclosures of PHI that is the Subject of the Disputed Amendment

1. If the patient submitted a statement of disagreement, the UEC will disclose all information listed in Item 5 above or an accurate summary of such information with all future disclosures of the PHI to which the disagreement relates.

2. If the patient did not submit a statement of disagreement, and if the patient has requested that the UEC provide the *Amendment of PHI* form and the amendment denial letter with any future disclosures, the UEC shall include these documents (or an accurate summary of that information) with all future disclosures of the PHI to which the disagreement relates.

Acceptance of the Request for Amendment

If the UEC accepts the requested amendment, in whole or in part, the UEC will take the following steps:

1. The UEC Privacy Officer shall place a copy of the amendment in the patient's Medical Record or provide a reference to the location of the amendment within the body of the Medical Record.

2. The Privacy Officer shall notify the relevant persons with whom the amendment needs to be shared, as identified by the patient on the original *Amendment of PHI* form.

3. The Privacy Officer shall identify other persons, including Business Associates that it knows have the PHI and that may have relied on, or could foreseeably rely on, such information to the detriment of the patient. The Privacy Officer will inform the patient of, and obtain the patient's agreement to notify such other persons or organizations of the amendment.

4. The Privacy Officer shall make reasonable efforts to inform and provide the amendment within a reasonable time to:

    a. Persons identified by the patient as having received the PHI and needing the amendment;
    b. Persons, including Business Associates, that the UEC knows have the PHI and may have relied, or could foreseeably rely, on such information to the detriment of the patient.

5. If no additional persons needing notification of the amendment are identified, the Privacy Officer shall inform the patient in writing that the amendment has been accepted.

Actions on Notices of Amendment

If another Covered Entity notifies the UEC of an amendment to PHI it maintains, the Privacy Officer shall make the amendment to the patient's Designated Record Set.

1. Amendments to the Designated Record Set shall be filed with that portion of the PHI to be amended.

2. Amendments that cannot be physically placed near the original PHI will be filed in an appropriate location.

3. If it is not possible to file the amendment(s) with that portion of the PHI to be amended, a reference to the amendment and its location will be added near the original information location.

4. If the actual amendment is not in an easily recognized location near the original information, the reference should indicate where it could be found.

5. General information regarding requests for amendment, forms relating to amendments and correspondence relating to denial or acceptance of requests to amend will be filed in the patient's Medical Record.

FERRIS STATE UNIVERSITY
University Eye Center

REQUEST TO AMEND

Part I: To be completed by Health Plan participant, covered spouse or covered dependent

1. Please complete the following:

Name: _____

Address: _____

Phone number: _____ Date: _____

Cell phone number: _____

Email Address: _____

Relation to patient: _____

Social Security number: _____ Date of birth: _____

2. This request concerns:

___ My health information.

___ The health information of my minor child who is covered by the Health Plan.

Child's name: _____ Child's SSN: _____ Child's date of birth: _____

___ The health information of an individual who is covered by the Health Plan and for whom I am the legal guardian.

___ Copies of documents establishing my legal authority are attached.

___ Copies of documents establishing my legal authority are already on file with the Heath Plan

Individual's name: _____ Individual's SSN: _____ Individual's date of birth: _____

3. I would like to amend the protected health information as follows:

Current entry: _____

_____

Date of entry: _____

Author of entry: _____

Corrected entry: _____

_____

Reason for corrected entry:
(attach supporting
documents) _____

4. I understand that this request and all supporting documents will be made a part of the record. I also warrant that I have truthfully represented my identity and that I am authorized to make this request, and understand that if I have misrepresented my identity or authority, that the University Eye Center may seek whatever criminal and civil relief is available.

_____ _____

Signature of participant Date

5. Submit this form to the Privacy Officer (MCO-101F).

Part II: To Be Completed By the Privacy Officer.

Received by: _____

Date received: _____

Extension requested: ☐ Yes ☐ No

Reason for extension: _____

Date extension notice sent (attach): _____

Date granted (attach):

Date PHI updated: _____

Where amended PHI was sent:

_____

Date denied (attached): _____

Reason for denial:
- ☐ PHI not created by the UEC
- ☐ Not permitted by federal law (i.e., Privacy Act, psychotherapy notes)
- ☐ PHI not a part of employee's designated record set
- ☐ PHI is accurate and complete
- ☐ Other:

_____

Date Statement of Disagreement filed (attach): _____

Date Rebuttal sent (attach):

Comments: _____

_____

_____

_____

Request processed by: _____

Federal law requires the retention of this document and all documents concerning this matter for a period of six years, beginning on the date of the final disposition of this request.

FERRIS STATE UNIVERSITY
University Eye Center

[patient address information]

Dear [name of patient]:

Thank you for your request dated [insert date] to amend information that we have about you. Unfortunately, we are unable to amend our information because:

[specify permitted reason]

If you are dissatisfied with our decision, you have two options.

1. You can write a statement disagreeing with our decision and explaining your point of view. We will keep this with your information, and include it in any authorized disclosure of your information from now on. We may decide to write a rebuttal to your statement of disagreement. If we do, it will be included with your information and sent along with any authorized disclosures of it from now on. If you want to do this, send your statement of disagreement to:

   Clinic Operations Supervisor

2. At your option, you could alternatively ask us to simply include your original amendment request with your information. If you do this, we will disclose your original request with any authorized disclosure of your information from now on. If you want to do this, call:

   Clinic Operations Supervisor

It is your right to complain to us or to the U.S. Department of Health and Human Services -- Office for Civil Rights if you feel that your privacy rights have been violated. If you want to complain to us, send a written complaint (either hard copy or electronic) to:

Clinic Operations Supervisor

Thank you, and we look forward to working with you in the future.

[signature block]

FERRIS STATE UNIVERSITY
University Eye Center

[patient address information]

Dear [name of patient]:

Thank you for your request dated [insert date] to amend information that we have about you. We have made the change that you requested. The corrected information will be sent whenever we are authorized to send your information to anyone from now on.

Please let us know if there is anyone who should get a copy of the corrected information right now. If there is, we will send the corrected information to them as quickly as possible.

We look forward to working with you in the future.

[signature block]

FERRIS STATE UNIVERSITY
University Eye Center

[patient address info]

Dear [name of patient]:

Thank you for your request to amend information that we have about you. Ordinarily, we would be able to respond to your request within 60 days, but due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by [insert farthest date].

We look forward to working with you in the future.

[signature block

Request for Alternative Confidential Communications

Purpose

To ensure the patient's right to request that communications of Protected Health Information ("PHI") be delivered by alternative means or at alternate locations.

Policy

A patient will be allowed to request that the UEC communicate PHI to him by alternative means or at alternative locations. The UEC shall accommodate reasonable requests.

Procedure

1. The patient will be notified of the right to request communication by alternative means or an alternative locations in the UEC's *Notice of Privacy Practices.*
2. The UEC Privacy Officer will manage requests to receive communications by alternative means.
3. When an inquiry is received from a patient regarding the right to request that the UEC communicate with him or his personal representative by some alternate means, the UEC will provide the patient with a copy of A *Request for Communications by Alternative Means* form. A request will not be evaluated until this request form is completed and signed by the patient or personal representative.
4. The Privacy Officer will review the completed *Request for Communications* form to determine if it is a reasonable request. The UEC may not require an explanation for the request. The UEC's decision will not be based on the perceived merits of the request. The UEC will accommodate a request determined to be reasonable.
5. The Privacy Officer will complete the Response section of the *Request for Communications* form to inform the patient of the UEC's decision.
6. The Privacy Officer shall maintain all requests and responses in the appropriate location in the patient's Medical Record.

FERRIS STATE UNIVERSITY
University Eye Center

REQUEST FOR ALTERNATIVE CONFIDENTIAL COMMUNICATIONS

Part I: To Be Completed By Health Plan Participant, Covered Spouse, or Covered Dependent

1. Please complete the following:

Name: _____

Address: _____

Phone number: _____ Date: _____

Cell Phone No.: _____

Email Address: _____

Relation to Patient: _____

Social Security number: _____ Date of birth: _____

2. This request concerns:

___ My health information.

___ The health information of my minor child who is covered by the Health Plan.

Child's name: _____ Child's SSN: _____ Child's date of birth: _____

___ The health information of an individual who is covered by the Health Plan and for whom I am the legal guardian.

___ Copies of documents establishing my legal authority are attached.

___ Copies of documents establishing my legal authority are already on file with the Heath Plan

Individual's name: _____ Individual's SSN: _____ Individual's date of birth: _____

3. I, _____, request that all of my protected health information be communicated in the following manner (please check the appropriate box):

- ☐ Fax
  Fax number: _____
- ☐ Telephone
  Phone number:
  _____
- ☐ Mail
  Address:_____
  _
  _____
  _
- ☐ E-Mail
  Address:_____
  _____
- ☐ Other:
  _____

4. Check if applicable

- ☐ I hereby certify that failure to disclose all or part of my protected health information as requested above could put me in danger.
- ☐ I hereby certify that failure to disclose all or part of my protected health information as requested above could put the individual for whom I am responsible in danger.

5. Signature. By signing this document, I hereby warrant that I have truthfully represented my identity and that I am authorized to make this request. I understand that if I have misrepresented my identity or my authority, that the University Eye Center may seek whatever criminal and civil relief is available.

Signature: _____ Date: _____

6. Submit this form to the Privacy Officer (MCO-101F).

Part II: To Be Completed By the Privacy Officer.

Received by: _____

Date received: _____

Status: ☐ Granted ☐ Denied

Request processed by: _____

Federal law requires the retention of this document and all documents concerning this matter for a period of six years, beginning on the date of the final disposition of this request.

Patient Requested Restrictions on Use and Disclosures of PHI

Purpose

To provide a process for a patient to request a restriction to an otherwise permitted use or disclosure of the patient's Protected Health Information ("PHI"), and for the UEC to respond to such request.

Policy

A patient has the right to request that otherwise permitted uses and disclosures of PHI be restricted. Specifically, the patient may request restrictions on:

- The use and disclosure of PHI for treatment, payment or health care operations, or
- The disclosures to family, friends or others for involvement in care and notification purposes.

Except as provided below, the UEC is not required to comply with such requests for restriction, but will consider and may agree to a restriction. The UEC will consider the need for access to PHI for treatment purposes when considering a request for a restriction. A request for restriction must be made in writing. The UEC Privacy Officer will notify the resident of its determination with respect to the request.

Procedure

1. The patient will be notified of the right to request restrictions on the use and disclosure of PHI in the UEC's *Notice of Privacy Practices* and that the request must be in writing.
2. The Privacy Officer shall manage requests for restrictions. All documentation associated with this request will be placed in the patient's Medical Record.
3. The Privacy Officer will provide the patient a *Request to Restrict Use and Disclosure of Protected Health Information* ("*Request to Restrict")* form if the patient asks to make a restriction.
4. A request for restriction will not be reviewed until the *Request to Restrict* form is completed and signed by the patient. The Privacy Officer may assist the patient in completing the form, if necessary.
5. The Privacy Officer will review the request in consultation with other UEC staff to determine the feasibility of the request. The UEC shall give primary consideration to the need for access to the PHI for treatment and payment purposes in making its determination.
6. The Privacy Officer shall complete the "UEC Response" section of the *Request to Restrict* form and provide a copy to the patient.

<u>Restriction Not Accepted</u>

1. If the UEC declines the request for restriction, the Privacy Officer will provide the patient with a copy of the signed response (part of the *Request to Restrict* form).

<u>Restriction Accepted</u>

1. If the UEC agrees to the requested restriction, it must abide by the accepted restriction with the following exceptions:
    a. The UEC may use the restricted PHI, or may disclose such information to a health care provider if:
    b. The patient is in need of emergency treatment, and
    c. The restricted PHI is needed to provide emergency treatment. In this case, the UEC will release the information, but ask the emergency treatment provider not to further use or disclose the patient's PHI.
2. The UEC may disclose the information to the individual who requested the restriction.

3. The UEC may use and disclose the restricted PHI when statutorily required to use and disclose the information under the HIPAA Privacy Rule.
4. The Privacy Officer will notify appropriate UEC staff of the restriction.
5. The Privacy Officer will document the restriction on the *Request to Restrict* form, provide the patient with a copy and maintain the original in the patient's Medical Record.

Restrictions on Dislosures to Health Plans
The UEC must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if:

1. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
2. The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the UEC in full.

Terminating the Restriction
Termination with the patient's agreement

1. The UEC may terminate the accepted restriction if:
    a. The patient agrees to the termination in writing; or
    b. The patient agrees to the termination verbally and the verbal agreement is documented.
2. The Privacy Officer will notify the appropriate UEC staff of the termination of the restriction.
3. The Privacy Officer will document the patient's agreement to the termination of the restriction on the *Request to Restrict* form, provide the patient with a copy and maintain the documentation in the patient's record.
4. Termination of a restriction with the patient's agreement is effective for all PHI created or received by the UEC.

Termination without the patient's agreement

1. The UEC may terminate the restriction without the patient's agreement if it informs the patient that the restriction is being terminated.
2. Such termination is only effective with respect to PHI created or received after the UEC has informed the patient that it is terminating the restriction.

Note: The UEC must continue to abide by the restriction with respect to any PHI created or received before it informed the patient of the termination of the restriction.

a. Inform by mail: If the patient is informed by mail that the UEC is terminating the restriction, the notification shall be sent via certified mail, return receipt requested. The UEC shall maintain a copy of the notification and of the return receipt with the *Request to Restrict* form. The UEC shall not terminate the restriction until it receives confirmation that the patient has received the notification.
b. Inform in person: It is preferable to have the patient sign and date a notification of termination of a restriction. However, it will be acceptable to document that the patient was so notified on the *Request to Restrict* form.
c. Inform via telephone: If the patient is informed by telephone, this action shall be documented on the *Request to Restrict* form. In addition, a letter shall be sent via certified mail, return receipt requested. The termination shall be effective as of the date the patient is informed by telephone.

FERRIS STATE UNIVERSITY
University Eye Center

REQUEST FOR ADDITIONAL RESTRICTIONS

Part I: To Be Completed By Health Plan Participant, Covered Spouse, or Covered Dependent

1. Please complete the following:

Name: _____

Address: _____

Phone number: _____ Date: _____

Cell phone No.: _____

E-Mail Address : _____

Relation to Patient : _____

Social Security number: _____ Date of birth: _____

2. This request concerns:

___ My health information.

___ The health information of my minor child who is covered by the Health Plan.

Child's name: _____ Child's SSN: _____ Child's date of birth: _____

___ The health information of an individual who is covered by the Health Plan and for whom I am the legal guardian.

___ Copies of documents establishing my legal authority are attached.

___ Copies of documents establishing my legal authority are already on file with the Heath Plan

Individual's name: _____ Individual's SSN: _____ Individual's date of birth: _____

3. I request that the following additional restrictions be placed on my protected health information (please check the appropriate box):

☐ Restrict use or disclosure of my protected health information to carry out treatment, payment, or health care operations as follows:

_____

_____

☐ Restrict disclosure of my protected heath information to a family member, other relative, close personal friend or other person identified by me that is directly relevant to such person's involvement with my health care or payment for my health care services as follows:

_____

☐ Restrict use or disclosure of my protected health information to notify or assist in notifying a family member, personal representative, or other person responsible for my care, of my location, general condition, or death as follows:

_____

_____

_

☐ Restrict use or disclosure of my protected health information to a public or private entity assisting in disaster relief efforts to notify or assist in notifying a family member, personal representative, or another person responsible for my care, of my location, general condition, or death as follows: _____

_____

4. Signature. By signing this document, I hereby warrant that I have truthfully represented my identity and that I am authorized to make this request. I understand that if I have misrepresented my identity or my authority, that the University Eye Center ("UEC") may seek whatever criminal and civil relief is available.

I understand that the UEC may deny this request. I also understand that if the UEC agrees to this request, my protected health information may not be used or disclosed for the reasons checked above, ***except*** in the event of an emergency where I need emergency treatment and my protected health information is necessary to provide such emergency treatment. In this event, the UEC may use or disclose restricted protected health information to a health care provider in order to provide such treatment. If this information is disclosed, the health care provider will be notified that he or she must not further use or disclose such information.

Signature: _____ Date: _____

5. Submit this form to the Privacy Officer (MCO-101F).

Part II: To Be Completed By the Privacy Officer.

Received by: _____

Date received: _____

Time received: _____

Status of request: Granted: _____ Denied: _____

If denied, reason for denial: _____

Date denial notice sent (attached): _____

Request processed by: _____

Federal law requires the retention of this document and all documents concerning this matter for a period of six years, beginning on the date of the final disposition of this request.

Accounting of Disclosures of PHI

Purpose

Patients have the right to receive an accounting of the disclosures of their Protected Health Information ("PHI") maintained in their Designated Record Set. The following is the process for responding to a patient's request for an accounting of disclosures of their PHI made by the UEC.

Policy

Each patient may request and receive an accounting of trackable disclosures of PHI made by the UEC. The potential areas where accounting of disclosures applies are listed in the *Notice of Privacy Practices*. The UEC will provide such an accounting, in accordance with the HIPAA Privacy Rule, when requested by a patient or a patient's personal representative. The requested information will not include PHI released or disclosed on or prior to April 13, 2003.

Records of disclosures are retained for as long as the record is retained by FSU.

Procedure

1. Upon receiving an inquiry from a patient, the UEC Privacy Officer provides the patient or personal representative with a copy of a *Request for an Accounting of Disclosures of PHI* (*"Request")* form.

   Requests are not evaluated until the *Request* form is completed and signed by the patient or personal representative.

2. The UEC Privacy Officer reviews and processes the request.

3. The UEC provides a written accounting no later than 60 days after receipt. If the UEC is unable to meet the 60-day time frame, the UEC may extend the time once by no more than 30 days as long as the individual is provided with a written statement of the reasons for the delay and the date by which the UEC will provide the accounting.

4. A written accounting is provided to the requestor using an *Accounting of Disclosures* log.

   a. The accounting will include disclosures during the period specified by the patient or personal representative in the request. The specified period may be up to six years prior to the date of the request.

   b. The UEC will include known disclosures made by its Business Associates, if aware of any such disclosures required to be included in an accounting.

   c. For each disclosure, the accounting will include:

      i. Date the request for disclosure was received;

      ii. Name of entity requesting disclosure and, if known, the address of such person or entity;

      iii. A brief description of the PHI that was disclosed; and

      iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

   d. If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, the UEC may provide:

      i. The first disclosure during the accounting period;

ii. The frequency, or number of disclosures made during the accounting period;

iii. The date of the last such disclosure during the accounting period.

5. For disclosures of PHI for research purposes in a project consisting of fifty or more individuals, the accounting may provide:

   a. Name of protocol or other research activity;

   b. Description and purpose of research, criteria for selecting particular records;

   c. Brief description of the type of PHI disclosed;

   d. Date or period of time during which disclosure(s) occurred, including date of last disclosure during accounting period;

   e. Name, address, telephone number of entity that sponsored the research and of the researcher to whom the information was disclosed;

   f. Statement that PHI of the patient may or may not have been disclosed for a particular protocol or the research activity.

6. The UEC will provide the first accounting to a patient or personal representative within a 12-month period without charge. However, the UEC may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same party within the 12-month period, provided the UEC has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.

7. The UEC may exclude those disclosures that qualify as an exception.

8. The UEC must document and retain for ten years from the date of the accounting:

   a. The information required to be included in the accounting, and
   b. The written accounting provided to the requesting party.

<u>Potential Areas where Accounting of Disclosures Applies:</u>

1. Disclosures to Public Health Authorities

- For the purpose of preventing or controlling disease, injury or disability
- To conduct public health surveillance
- For public health investigations and interventions
- For reporting vital events such as births and deaths
- To a foreign government agency at the request of a public health authority
- To report child/elder abuse
- If necessary, to prevent or lessen a serious and imminent threat to the health or safety of an patient or the public

2. Disclosures to an Entity Subject to the Food and Drug Administration

- To report adverse events, product defects or biological product deviations
- To track products
- To enable product recalls, repairs or replacements
- To conduct post marketing surveillance

3. Disclosures to an Employer

- Only PHI specific to a work-related illness or injury, and
- Required for the employer to comply with its obligations under federal or state occupational safety and health laws

4. Disclosures to Health Oversight Agencies

- For government benefit program eligibility
- To determine compliance with civil rights laws
- For civil, administrative or criminal investigations, proceedings or actions

5. Disclosures in Judicial and Administrative Proceedings

- In response to a court order or court ordered warrant
- In response to a subpoena once approved by FSUs General Counsel

6. Disclosures to Law Enforcement Officials

- For the purpose of locating a suspect, fugitive, material witness or missing person
- About a patient who is or is suspected to be a victim of a crime
- Regarding crimes on the UEC or FSU premises
- Regarding suspicious deaths
- In response to an administrative request, civil investigative demand or grand jury subpoena, after approval by General Counsel
- For the purpose of averting a serious threat to health or safety

7. Disclosures about victims of abuse, neglect or domestic violence

- To a government authority authorized by law to receive reports of abuse, neglect or domestic violence

8. Disclosure of Deceased Persons' PHI

- To the Coroner, Medical Examiner or Funeral Directors
- To organ procurement organizations

9. Disclosures for research

- Only if disclosure was made without an authorization as permitted by the Privacy rule

10. Disclosures for Specialized Government Functions

- To Armed Forces personnel for military purposes
- To authorized federal officials for the protection of the President and other Federal officials
- To other government agencies, if approved by General Counsel

11. Disclosures for Worker's Compensation

- As authorized by and to the extent necessary to comply with the law

<u>Exceptions to Accounting of Disclosures:</u>
Accounting of disclosure does not include disclosures:

- Necessary to carry out treatment, payment, and health care operations
- To the patient for whom the PHI was created or obtained
- Pursuant to a signed authorization by the patient or personal representative
- For persons involved in the patient's care or other notification purposes
- For national security or intelligence purposes
- To a correctional institution
- That are incidental
- As part of a Limited Data Set

-

ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION
In Response to Request for Accounting

Patient's Name:_____ Medical Record Number:_____

Student Number: _____

Date Provided: _____

Date Requested: _____

Fee for Service: _____

Name of Entity Requesting Disclosure	Address of Entity Requesting Disclosure	Brief Description of PHI Disclosed	Purpose of Disclosure	Date Disclosed

Signature of Privacy Officer: _____

Distribution of copies: Original to resident's Medical Record, copy to Patient

FERRIS STATE UNIVERSITY
University Eye Center

REQUEST FOR AN ACCOUNTING OF DISCLOSURES

Part I: To Be Completed By Health Plan Participant

1. Please complete the following:

Name: _____

Address: _____

Phone number: _____ Date: _____

Cell Phone No: _____

Email: _____

Relation to patient:

_____ _____

Social Security number: _____ Date of birth: _____

2. This request concerns:

___ My health information.

___ The health information of my minor child who is covered by the Health Plan.

Child's name: _____ Child's SSN: _____ Child's date of birth: _____

___ The health information of an individual who is covered by the Health Plan and for whom I am the legal guardian.

___ Copies of documents establishing my legal authority are attached.

___ Copies of documents establishing my legal authority are already on file with the Heath Plan

Individual's name: _____ Individual's SSN: _____ Individual's date of birth: _____

3. Time frame for accounting of disclosures. NOTE: You can request an accounting of disclosures for dates up to 6 years prior to the date of your request, or disclosures made on or after September 23, 2013, whichever date is more recent.

From: _____ To:_____

4. Fees: There is no charge for the first accounting request in a 12-month period. For subsequent requests in the same 12-month period, the University Eye Center ("UEC") may charge for its costs in providing the accounting.

This is my (please initial):

_____ First request within 12 months (please initial).

_____ Second (or more) request within 12 months. I understand that I may be charged a fee, and if so, someone from the employee benefits department will contact me with an estimate of the costs, and at that time I may decide to withdraw or modify this request.

5. Signature. By signing this document, I hereby warrant that I have truthfully represented my identity and that I am authorized to receive the information that I have requested. I understand that if I have misrepresented my identity or my authority, that the UEC may seek whatever criminal and civil relief is available.

_____ _____

Signature of individual Date

6. Submit this form to the Privacy Officer (MCO-101F).

Part II: To Be Completed By the Privacy Officer.

Received by: _____

Date received: _____

Time received: _____

Extension requested: ☐ Yes ☐ No

Reason for extension: _____

Date extension notice sent (attached): _____

Date accounting sent (attached): _____

Request processed by: _____

Federal law requires the retention of this document and all documents concerning this matter for a period of six years, beginning on the date of the final disposition of this request.

FERRIS STATE UNIVERSITY
University Eye Center

[patient address info]

Dear [name of patient]:

Thank you for your request dated [specify date] for an accounting of disclosures that we have made of your protected health information. Ordinarily, we would provide this accounting to you within 60 days of receipt of your written request. Unfortunately, we are unable to provide your accounting within this time because [specify reason]. We will have your accounting ready by [specify date].

Thank you for your patience, and we look forward to working with you in the future.

[signature block]

University Eye Center
Breach Notification Policy

1. Breach Notification Team.

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

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

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

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

2. Investigation

In the event the Information Technology Department or a member of Ferris State's workforce detects or otherwise learns of a security violation of its electronic or paper files, it will conduct an investigation of the security incident consistent with its Policies and Procedures. If the incident involves records containing PHI, the Information Technology Department will notify the Privacy Officer of the health care component where the violation may have occurred. Other workforce members who learn of an incident involving unauthorized access to PHI (whether in electronic or paper form) will also notify the Privacy Officer of the health care component where the violation may have occurred of the incident.

Upon notification of a potential incident of unauthorized access to PHI, the Privacy Officer of the health care component where the violation may have occurred will determine whether Ferris State has a duty to notify individuals about a breach. In determining whether notification is required, the Privacy Officer of the health care component where the violation may have occurred may consult with legal counsel, employees, agents, contractors or consultants as reasonably necessary to determine Ferris State's notification obligations, if any.

3. Determine whether a breach has occurred.

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

- Ferris State learns that an unauthorized individual has gained access to Ferris State's electronic information system.

- Ferris State learns that an authorized individual may have accessed protected health information for an improper purpose.

- Ferris State learns that information intended for an authorized individual was misdirected (for example, by e-mail or fax transmission).

- Ferris State learns that a business associate has suffered a potential data breach.

- Ferris State hears from individuals who are the subject of protected health information that they have been the victims of identity theft or other identity fraud crime.

- Ferris State learns that a client file that may contain sensitive information cannot be located.

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

- The specific data that is involved in the incident.

- Whether the access, use or disclosure is consistent with Ferris State's HIPAA policies and procedures.

- The manner in which the information was accessed, used or disclosed, and the circumstances surrounding the incident.

- The date the incident was discovered.

- The date(s) the incident occurred.

- The number of individuals whose information was involved.

- The states in which the individuals reside.

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

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

Note: while much of this policy addresses breach notification requirements under HIPAA, most states have security breach notification requirements that may also apply. Therefore, the Breach

Notification Team may need to consult with legal counsel to determine if Ferris State has any obligations under state notification laws—whether or not notification is required under HIPAA.

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

A. Determine whether the information is deemed "secured" under HIPAA.

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

- If the information is electronic, the data is considered secured if *both* of the following are true:

    1. The data has been properly encrypted consistent with guidance issued by the Department of Health & Human Services. This guidance may change from time to time, but as of September 2009, HHS guidance called for the following:

        - For data at rest (including data that resides in databases, file systems, flash drives, memory and other structured storage methods), the encryption process must be consistent with National Institute of Standards & Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*

        - For data in motion (which includes data moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange), the encryption process must comply, as appropriate, with one of the following:

            - National Institute of Standards & Technology Special Publication 800-52, *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.

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

- Data that has been destroyed may also be considered secured if one of the following is true:

1. The information was stored on paper, film or other hard copy media, and the media has been shredded or destroyed in such a way that the protected health information cannot be reconstructed. (Note that redaction is **not** an effective form of destruction.)

2. The information is in electronic form and has been cleared, purged or destroyed consistent with National Institute of Standards & Technology Special Publication 800-88, *Guidelines for Media Sanitization*, so that the protected health information cannot be retrieved.

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

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

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

If the information is not considered secured, the incident may still not be considered a breach if the incident falls within one of the following exceptions:

1. Unintentional acquisition, access or use of protected health information. In order for this exception to apply, all of the following have to be true:

    a. the unauthorized acquisition, access or use of protected health information must have been unintentional;

    b. the individual who acquired, accessed or used the protected health information must be one of the following:

- a member of Ferris State's workforce
- A member of a business associate's workforce
- A person acting under the authority of Ferris State or Ferris State's business associate

    c. The individual who acquired, accessed or used the protected health information did so in good faith.

    d. The acquisition, access or use did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

2. Inadvertent internal disclosure of protected health information. This exception applies if all of the following are true:

    a. The disclosure is made by an individual who is authorized to access protected health information

b. The disclosure is made to an individual who is authorized to access protected health information.

c. Both individuals work for the same organization, which may be one of the following:

- Ferris State
- Ferris State's business associate
- An organized health care arrangement in which Ferris State participates.

d. The disclosure did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

3. Where the information would not be retained. This exception applies if all of the following are true:

a. The disclosure is made to an unauthorized individual.

b. Ferris State or its business associate has a good-faith belief that the unauthorized individual would not reasonably have been able to retain the information.

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

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

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

Factors to consider include:

- The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification.
  - Did it include social security numbers, driver's license numbers, bank account/credit card numbers, insurance numbers, or other sensitive information that could be used for identity theft or identity fraud crimes?
  - Did it include information about medical treatment, diagnoses, diseases, or similar details about an individual's health?

        - What is the likelihood that the Protected Health Information could be reidentified based on the context and the ability to link the information with other available information?

    - The unauthorized person who used the Protected Health Information or to whom the disclosure was made.

        - Was the recipient also a HIPAA covered entity with a legal duty not to misuse the information?

        - Does the recipient have a contractual relationship with Ferris State that prohibits it from misusing the information?

        - Are there other facts and circumstances that would indicate that the recipient of the information is unlikely to misuse the information?

    - Whether the Protected Health Information was actually acquired or viewed.

        - Does a forensic analysis indicate that Protected Health Information on a lost computer was never accessed, viewed, acquired, transferred or otherwise compromised??

    - The extent to which the risk to the PHI has been mitigated.

        - Are there past dealings with the recipient or other factors that would indicate that the recipient can be trusted not to use or further disclose the information?

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

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

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

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

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

the Breach Notification Team will work with the business associate to determine whether the incident requires notification.

5. Notification

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

A. Notice to Individuals

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

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

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

All notifications must be written in plain language.

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

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

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

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

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

Note: State security breach notification laws may also apply and may mandate a shorter time frame for notification.

If Ferris State does not have sufficient contact information for some or all of the affected individuals (or if the contact information is outdated) then Ferris State must provide substitute notice for such individuals in the following manner:

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

- If more than 10 individuals are affected, HIPAA requires the following:

    - a conspicuous posting for a period of 90 days on Ferris State's home page **or** a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside; and

    - a toll-free phone number active for 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

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

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

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

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

B. Notice to the Media

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

Note: State security breach notification laws should also be consulted to determine whether there are additional notification obligations to the media, state agencies, or national credit bureaus.

Ferris State must retain copies of all press releases provided to prominent media outlets for at least six years from the date the notifications were provided.

C. To the Department of Health & Human Services

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

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

- If the breach involves fewer than 500 individuals:

    - The Privacy Officer of the health care component where the violation may have occurred must maintain a log of notifications involving fewer than 500 individuals. The information to be recorded in the log will be set forth on the Department of Health & Human Services' Web site.

    - The Privacy Officer of the health care component where the violation may have occurred, in coordination and consultation with the General Counsel's Office, will submit the log to the Department of Health & Human Services for each calendar year by February 28 of the following year, in the manner specified on the Department's Web site.

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

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

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

To the extent not addressed in the business associate agreement, Ferris State will use the following default rules set forth in HIPAA:

- Ferris State will notify the covered entity as soon as possible after discovering a potential breach, and no later than 60 days after discovery.

- Ferris State will provide the covered entity with the following information, either at the time Ferris State provides notice of the potential breach to the covered entity or promptly thereafter as the information becomes available:
    - The identity of each individual whose unsecured protected health information has been, or is reasonably believed to have been, breached, to the extent possible.
    - Any other available information that the covered entity is required to include in the notification to the individual. This may include the following:
        - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
        - A description of the types of unsecured protected health information that were involved in the breach.
        - Any steps the individual should take to protect themselves from potential harm resulting from the breach.
        - A brief description of what Ferris State is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
        - Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.
- Ferris State will cooperate with covered entity in determining whether notification is required under HIPAA.

END