Health Insurance Portability and Accountability Act

Policies and Procedures Compliance Manual

Human Resources

Ferris State University

Introduction to Ferris State University's HIPAA Privacy Policies and Procedures

Privacy regulations under HIPAA—the Health Insurance Portability and Accountability Act of 1996—require Ferris State University ("FSU") to protect the privacy of individually identifiable health information of participants in FSU's health plans (the "Health Plan"). This information is known as protected health information, or "PHI" for short.

FSU's policy is to fully comply with HIPAA's privacy requirements (the "Privacy Rules"). All members of FSU's workforce who use or have access to PHI must comply with the policies and procedures set forth herein ("Policies and Procedures"). Failure to comply will result in disciplinary action as set forth in FSU's employment handbook. For purposes of these Policies and Procedures, FSU's workforce includes employees, volunteers, trainees, and other persons whose work performance is under the direct control of FSU, whether or not they are paid by FSU.

FSU does not intend to create any third party rights (including rights of Health Plan participants, beneficiaries, covered dependents or outside service providers) by adopting these Policies and Procedures. FSU may amend or change these Policies and Procedures at any time, even retroactively, without notice. FSU intends that these Policies and Procedures implement HIPAA's Privacy Rules and will interpret them consistent with the regulations promulgated under HIPAA. To the extent that these Policies and Procedures establish requirements and obligations beyond those required by HIPAA, they are aspirational and not binding upon FSU. These Policies and Procedures do not address requirements under other federal, state, or local laws.

Table of Contents

PRIVACY POLICIES AND PROCEDURES

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

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

PHI (Protected Health Information): PHI is individually identifiable health information about an individual that relates to the past, present or future physical or mental health or condition of the individual. PHI includes not only information about health care treatment that individuals receive, but also information about whether they are covered by the Health Plan, what their Health Plan payments are, and who else in their family is covered. If the information identifies the person, or can be used to identify the person, then it is PHI. To qualify as PHI, the information must be related to the Health Plan.

PHI does not include enrollment information found in FSU's employment records (whether held by FSU or its enrollment administrator). Enrollment information is defined under HIPAA Transaction standards, but is generally information such as name, address, social security number, elected coverage and cost of coverage. However, enrollment information will be considered PHI when it is in the hands of the Health Plan's third party administrators and in FSU's health plan records.

PHI includes information in written, oral, or electronic form. It includes information that you obtain as a result of working with the Health Plan. PHI must be kept confidential. You should not discuss it with anyone, except as necessary to perform your duties related to the Health Plan.

Information about an individual is no longer considered PHI once the individual has been deceased for more than 50 years. Therefore, FSU is not obligated to apply these Policies and Procedures to Health Plan information about an individual who has been deceased for more than 50 years.

Limited Data Set: A Limited Data Set is PHI that has had most identifiers of the individual, or of relatives, employers, or household members removed from it. A Limited Data Set is similar to De-identified Information (see below), except that a Limited Data Set may include city, state and zip code information and any dates related to an individual. Limited Data Set is further defined at 45 C.F.R. § 164.514(e).

Minimum Necessary: The Privacy Rules require that when PHI is used or disclosed, you must make reasonable efforts to limit the use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. For example, if someone asks for an individual's Health Plan records in order to perform a function on behalf of the Health Plan, but the records include more information than is really needed for that particular function,

you should disclose only the information needed (and not the entire record). (See Section V, "Procedures for Complying with the "Minimum Necessary" Standard.)

Workforce/Employee: FSU's workforce means any individual who works directly under the control of FSU, whether or not they are paid by FSU. This includes not only employees, but also volunteers, trainees, interns/externs, workers employed by a temporary agency, and independent contractors. Whenever the Policies and Procedures discuss FSU's obligation to protect PHI, the discussion is intended to include anyone who is a member of FSU's workforce. The term "employee" when used in the Policies and Procedures means any member of FSU's workforce.

Designated Record Set: "Designated record set" means the enrollment, payment, claims adjudication and other records that are maintained by the Health Plan. It includes records that are maintained on behalf of the Health Plan, such as by a third party administrator or some other outside company that performs services for the Health Plan. It also includes records that may be used, in whole or in part, by or for the Health Plan to make decisions about an individual. For purposes of this definition, "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Health Plan.

Covered Entity: "Covered Entity" means an individual or entity that is subject to the Privacy Rules. Covered Entity includes a health plan, health care clearinghouse, and health care provider who transmits any health information in electronic form in connection with a transaction covered by the Standards for Electronic Transactions (45 CFR 162.100 *et seq.*)

Use: "Use" of PHI means the sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any person working for, in connection with, or within FSU's human resources department, or by a business associate (as defined below) of the Health Plan.

Disclosure: "Disclosure" of PHI means the release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within FSU's human resources department.

Business Associate*:* A "business associate" is a person (other than a member of FSU's workforce) or entity that creates, receives, maintains or transmits PHI on behalf of the Health Plan. A business associate arranges, performs or assists in the performance of functions or activities for the Health Plan that involve PHI. Such functions include:

- claims processing or administration
- data analysis, storage, processing or administration
- utilization review
- quality assurance
- billing

- benefit management
- re-pricing
- any other function or activity regulated by HIPAA

A business associate also includes a person (other than a member of FSU's workforce) or entity that provides the following types of services, if the services involve the disclosure of PHI:

- legal
- actuarial
- accounting
- consulting
- data aggregation
- management
- administration
- accreditation
- financial services

De-identified Information*:* Information qualifies as "de-identified information" only if it does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. PHI can become de-identified in two ways:

- professional statistical analysis has determined that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; or
- 18 defined identifiers of the individual or of relatives, employers, or household members of the individual are removed

Payment*:* "Payment" means activities undertaken to obtain Health Plan premiums or to determine or fulfill the Health Plan's responsibility for coverage and provision of benefits, or to obtain or provide reimbursement for the provision of health care. Payment includes:

- determinations of eligibility or coverage, including coordination of benefits or the determination of cost sharing amounts
- adjudication or subrogation of health benefit claims

- risk adjusting amounts due based on enrollee health status and demographic characteristics

- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing

- review of health care services for purposes of determining coverage

Health Care Operations: "Health care operations" means any of the following activities to the extent that they are related to Health Plan administration:

- evaluating Health Plan performance

- underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits

- ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance)

- conducting quality assessment and improvement activities

- conducting or arranging for medical review, legal services, and auditing functions

- business planning and development

- business management and general administration activities

II. Health Plan's Responsibilities as a Covered Entity

A. <u>Privacy Officer and Contact Person</u>

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

- the Privacy Officer, who has overall responsibility for the privacy and security of PHI. The Privacy Officer is the Associate Vice President for Human Resources, and may be reached at 231/591-2150.

B. Workforce Training

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

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

C. Safeguards

The Privacy Rules require FSU to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. FSU's policy is to maintain appropriate safeguards as required by the Privacy Rules.

Administrative Safeguards. FSU's Policies and Procedures include numerous administrative safeguards to protect the privacy of PHI. These administration safeguards include:

- **appointment of the Privacy Officer to implement and oversee compliance with the Policies and Procedures**
- **distribution of a Notice of Privacy Practices to all Health Plan participants**
- **training of workforce members regarding the Policies and Procedures**
- **creation of administration firewalls between FSU's Health Plan functions and its employment functions**
- **establishment of a system to administer individual rights under the Health Plan (e.g., right to request additional privacy protection for PHI, right to inspect and copy PHI, right to request correction of PHI, right to notice of disclosures made by the Health Plan, and right to request confidential communication)**

- **establishment of a complaint system for individuals to use if they believe a privacy violation has occurred**

Technical Safeguards. FSU has adopted the following technical safeguards to protect the privacy of PHI on its computer systems:

- restriction of access to PHI on its computer systems to individuals who need access to PHI in order to perform their duties
- use of passwords to authenticate an individual's right to access PHI
- **creation of computer firewalls around PHI to protect it from unauthorized access by others within FSU or outside of FSU**
- changing of computer passwords on a routine basis

Physical Safeguards. FSU has adopted the following physical safeguards to protect the privacy of PHI:

- paper files containing PHI are kept in locked file cabinets
- only employees with responsibility for the Health Plan have access to Health Plan records; employees who do not have Health Plan responsibilities are not given access to Health Plan records
- portable media (such as diskettes, CDs, and computer tapes) are stored in secure locations where access is limited to authorized personnel
- main frame systems and servers storing PHI are kept in rooms with restricted access
- Health Plan records are kept separate from employment records
- Electronic Health Plan information is accessible only by employees with responsibility for the Health Plan who need access to such information. This includes electronic health information maintained internally (e.g., FSU information systems) and externally (e.g., third party administrator websites)
- reasonable precautions are taken to ensure that Health Plan records are not left out in the open or unattended
- Health Plan information is used only for Health Plan purposes; it is not shared for making employment decisions (hiring, firing, promotions, etc.) or for administering any non-health plan programs (e.g., workers' compensation, FMLA, disability, employee recognitions, etc.)

- FSU has made modifications to the physical layout of Human Resources with restricted access during and after business hours.

D. Complaints

The Privacy Rules require FSU to implement a process by which individuals may file complaints about privacy violations. FSU's policy is that anyone who believes that the Policies and Procedures or the Privacy Rules have been violated at FSU may submit a written complaint to the Privacy Officer.

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

- review the Policies and Procedures or Privacy Rules at issue
- obtain any additional information from the individual necessary to understand the nature and basis of the complaint
- investigate the conduct that is the subject of the complaint, which may include interviewing members of the workforce and business associates, and reviewing records in the individual's designated record set
- if appropriate, consult with legal counsel or other appropriate resources for evaluating the complaint
- decide how the complaint will be handled and then take appropriate action, which may include:
    - actions necessary to minimize any harmful effects from the unauthorized use or disclosure
    - disciplinary action against employees in accordance with FSU's disciplinary policies (see section II.E, "Discipline")
    - appropriate actions with respect to business associates in accordance with the relevant business associate agreement (see section III.I, "Uses and Disclosures of PHI by Business Associates")
    - modification of the Policies and Procedures, if necessary
    - no action, if it is determined that there has been no violation of the Policies and Procedures or the Privacy Rules
- communicate to the individual, in writing and on a timely basis, the final outcome of the complaint investigation

- retain documentation of the complaint and its disposition as required by the Privacy Rules' documentation requirements (see section III.M, "Documentation and Record Retention Requirements")

- complete the *Complaint Tracking Form*

E. Discipline

The Privacy Rules require FSU to have and apply appropriate discipline to employees who fail to comply with the Policies and Procedures or the Privacy Rules. FSU's policy is to appropriately discipline any employee who violates the Policies and Procedures or the Privacy Rules.

Type of Discipline. FSU will appropriately discipline employees who fail to comply with the Policies and Procedures or the Privacy Rules, in accordance with the disciplinary policies set forth in FSU's employee handbook, FSU's policies and procedures, and Collective Bargaining Agreements. Discipline will vary depending on the nature of the employee's misconduct, but discipline includes sanctions up to and including termination of employment.

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

- the employee believes in good faith that the Health Plan or FSU has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Health Plan or FSU potentially endangers one or more patients, workers, or the public; and

- the disclosure was made to the individuals or agencies and for the purposes set forth in the whistleblower provisions of the Privacy Rules (see section 164.502(j) of the Privacy Rules)

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

F. No Intimidating or Retaliatory Acts

The Privacy Rules prohibit FSU from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against individuals for exercising their rights under the Privacy Rules. FSU's policy is that FSU will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their privacy rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Rules.

G. No Waiver of Rights

The Privacy Rules prohibit FSU from requiring individuals to waive their individual rights under the Privacy Rules. FSU's policy is that individuals shall not be required to waive their rights under the Privacy Rules as a condition of treatment, payment, enrollment in the Health Plan, or eligibility for benefits.

Limited Exception for the Health Plan's Eligibility or Enrollment Determinations. FSU may condition enrollment in the Health Plan or eligibility for benefits on provision of an authorization requested by the Health Plan prior to an individual's enrollment in the Health Plan if (1) the authorization is sought for the Health Plan's eligibility or enrollment determination relating to the individual or for its underwriting or risk rating determinations; and (2) the authorization is not for a use or disclosure of psychotherapy notes.

H. Notice of Privacy Practices

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

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

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

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

Delivering the Notice. The Privacy Officer will ensure that that Notice is delivered to participants in the Health Plan as follows:

- to each new enrollee in the Health Plan at the time of the individual's enrollment
- If there is a material revision to the Notice:
    - if FSU posts its Notice of Privacy Practices on its web site and makes the notice electronically available, FSU will prominently

post the change or the revised Notice of Privacy Practices on its web site by the effective date of the material change to the Notice of Privacy Practices, and provide the revised Notice of Privacy Practices, or information about the material change and how to obtain the revised Notice in its next annual mailing to individuals covered by the Health Plan

- If FSU does not post its Notice of Privacy Practices on its website, FSU must provide the revised Notice of Privacy Practices, or information about the material change and how to obtain the revised Notice of Privacy Practices to individuals covered by the Health Plan within 60 days of any material revision to the Notice to individuals who are then covered by the Health Plan (unless HIPAA regulations allow for an alternative distribution schedule)

At least once every three years, the FSU will inform all participants then covered by the Health Plan that the Notice is available and how they can obtain a copy. FSU will also provide a copy of the Notice to any individual upon request.

Posting the Notice on FSU's Web Site. FSU maintains a web site that provides information about customer services or benefits (including an intranet site with information on employee benefits, the Health Plan, etc.), FSU must prominently post the Notice on the web site and make the Notice available electronically through the web site.

Electronic Delivery of Notice of Privacy Practices. The following rules apply to provision of the Notice of Privacy Practices by e-mail:

- If an individual agrees, the Notice of Privacy Practices may be delivered electronically by e-mail.

- An individual may withdraw permission to receive the Notice of Privacy Practices by e-mail at any time.

- If FSU knows that an e-mail transmission to an individual has failed, FSU must provide a paper copy of the Notice of Privacy Practices to the individual.

Revisions to the Notice. FSU will revise the Notice whenever there is a change in law that requires a material revision to the Policies and Procedures, or whenever FSU elects to make a material revision to the Policies and Procedures. When this occurs, FSU will redistribute the Notice to Health Plan participants.

III. Procedures for Uses and Disclosures of PHI

A. <u>Who Must Comply with These Policies and Procedures</u>

All members of FSU's workforce must comply with the Policies and Procedures. However, only members of FSU's workforce who assist in administering the Health Plan have access to PHI.

B. Limitations on Access to PHI

FSU limits access to PHI to employees with certain job functions ("Authorized Employees"). These Authorized Employees either perform functions directly on behalf of the Health Plan, or they access PHI on behalf of FSU for its use in administering the Health Plan. Authorized Employees are:

- Privacy Officer
- Director, Human Resources
- Benefits Manager
- Benefits Specialist
- HRIS Coordinator
- Administrative Assistant, Human Resources
- Others authorized or designated by the Associate Vice President for Human Resources

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

C. Permitted Uses and Disclosures of PHI for Payment and Health Care Operations

Although uses and disclosures of PHI are generally prohibited without an authorization, the Privacy Rules permit certain types of uses and disclosures for payment and health care operations without an authorization. FSU's policy is to disclose PHI for payment and health care operations as permitted in the Privacy Rules.

Uses and Disclosures for the Health Plan's Own Payment Activities or Health Care Operations. FSU may use and disclose an individual's PHI to perform the Health

Plan's own payment activities or health care operations. As permitted under the Privacy Rules, including, but not limited to the following activities:

- determining Health Plan benefits and eligibility for benefits
- paying claims and providing benefits
- enrollment and disenrollment in benefit programs
- obtaining premium bids and quotes for administrative services, and other activities related to placement, renewal or replacement of a contract of health insurance or for administration of health benefits (including stop-loss and excess loss insurance)
- determining costs of self-insured benefits and employee contribution amounts
- coordinating benefits with other plans and coverages
- final adjudication of appeals on claims appeals
- exercise of the Health Plan's rights of recovery, reimbursement, and subrogation
- obtaining employee contributions
- assisting participants and beneficiaries with questions relating to eligibility, benefits, appeals and other inquiries relating to the Health Plan
- evaluating plan performance and making recommendations to Amway on Health Plan design issues
- engaging in quality assessment activities
- complying with laws that apply to the Health Plan, such as ERISA, COBRA, Medicare Secondary Payer rules, etc.
- obtaining legal services relating to the administration of the Health Plan
- performing auditing functions, including programs to detect fraud and abuse
- engaging in cost-management activities
- making claims under stop-loss or excess loss insurance

- engaging in business planning, management and other general administration of the Health Plan

- conducting activities in connection with the transfer, merger or consolidation of the Health Plan, including due diligence.

In doing so, FSU must follow these procedures:

- *Routine Uses and Disclosures*. Routine payment and health care operations may be performed without approval of the Privacy Officer.

    - in performing these routine functions, FSU must follow its departmental policies and procedures (see section V.E., "Department Minimum Necessary Policies and Procedures").

    - each such use or disclosure must be limited to the minimum necessary to achieve the purpose of the disclosure (see section V, "Procedures for Complying with the Minimum Necessary Standard")

- *Non-routine Uses and Disclosures*. Non-routine uses or disclosures must be approved by the Privacy Officer, who will approve a non-routine use or disclosure only after considering FSU's use and disclosure criteria (see section V)

Disclosures for Another Covered Entity's Payment Activities. FSU may disclose an individual's PHI to another covered entity or health care provider so that the other covered entity or health care provider may perform payment activities. Such disclosures must be made in accordance with the following:

- *Routine Disclosures*. Routine disclosures may be performed without approval of the Privacy Officer

- *Non-routine Disclosures*. Non-routine disclosures must be approved by the Privacy Officer, who will approve a non-routine disclosure only after consideration of FSU's disclosure criteria (see section V)

Disclosures for Certain Health Care Operations of the Receiving Covered Entity. FSU may disclose PHI for purposes of another covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if

- the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship

- the disclosure complies with the minimum necessary standard (see section V)

- the disclosure is approved by FSU's Privacy Officer, who will approve the disclosure only after consideration of FSU's disclosure criteria (see section V)

Uses and Disclosures for Plans or Programs Other than the Health Plans. Unless an individual who is the subject of the PHI has provided an authorization, FSU may not use or disclose the individual's PHI for the payment or administration of FSU's plans or programs other than the Health Plan (e.g., disability, worker's compensation, life insurance, etc.).

If FSU needs an individual's PHI for the payment or administration of FSU plans or programs other than the Health Plan, the following procedures must be followed:

- obtain an authorization from the individual
    - contact the Privacy Officer to determine whether an authorization for this type of use or disclosure is already on file. The authorization must allow the particular use or disclosure at issue
    - if no authorization is on file, request the *Individual Authorization Form* from the Privacy Officer. Because the Privacy Rules require authorizations to meet specific content requirements, FSU shall use the *Individual Authorization Form* unless the Privacy Officer specifically approves otherwise
- the Privacy Officer must approve the use or disclosure after considering FSU's use and disclosure criteria (see section V)
- the use or disclosure must comply with the minimum necessary standard (see section V)

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

Use of Genetic Information. FSU will not use any genetic information, including family medical history, to conduct any eligibility determinations or other underwriting activities. This includes the computation of premiums or contribution amounts under the Health Plan.

D. Mandatory Disclosures of PHI to Individuals and HHS

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

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

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

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

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

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

- FSU's Privacy Officer approves the use or disclosure after consultation with legal counsel
- the disclosure complies with the minimum necessary standard or is specifically exempted from the minimum necessary standard (see section V, "Procedures for Complying with the Minimum Necessary Standard")
- the disclosure falls within one of the following categories, and the specific requirements set forth in the Privacy Rules have been followed (see section 164.512 of the Privacy Rules):
    - in response to an order of a court or an administrative tribunal
    - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, provided that there is an appropriate protective order in place and, where medical records are involved, the individual has waived his or her physician-patient privilege
    - pursuant to process (such as a court-ordered warrant or an administrative summons) and as otherwise required by law
    - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual

who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on FSU premises

- about an individual that FSU reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information
- to appropriate public health authorities for public health activities
- to a health oversight agency for health oversight activities
- to coroners, medical examiners, and funeral directors about a deceased individual
- for cadaveric organ, eye or tissue donation purposes
- for certain research purposes, when the need for an authorization has been waived or is otherwise not required
- in order to avert a serious threat to health or safety
- about armed forces personnel to appropriate military command authorities
- for national security and intelligence activities
- for protective services to the President of the United States and other designated persons
- to correctional institutions and law enforcement custodians
- in connection with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault

- if the disclosure is to a public official, verify the identity of the public official using the procedures set forth in "Verifying the Identity of Those Requesting Potential Health Information" (see section III.L)
- 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 FSU receives a subpoena, FSU may not release a party's medical records without an accompanying court order, administrative order, or patient's waiver of the physician-patient privilege (see Mich. Ct. Rule 2.314)
- document the disclosure according to the Privacy Rules' documentation requirements (see section III.M, "Documentation and Record Retention Requirements"), except that documentation is not required if the disclosure is for:

- national security or intelligence purposes; or
- to correctional institutions or law enforcement custodians

F. Use of PHI for Marketing

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

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

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

Exceptions. The definition of marketing expressly excludes refill reminders or other communications about a drug or biologic currently prescribed to someone enrolled in the Health Plan. Therefore, such communications do not require an individual's authorization—even if FSU (or FSU's business associate) receives payment from a third party (such as a pharmaceutical) for making such communications, so long as the payment received from the third party is reasonably related to FSU's (or its business associate's) cost of making the communication.

Marketing also does not include communications made for the following purposes, *unless* 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.

G. Sale of PHI

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

Definition. "Sale of PHI" means any disclosure of PHI where FSU 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 FSU 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 FSU 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 FSU and related due diligence.
- To a business associate for activities that the business associate undertakes on behalf of FSU, if the only remuneration is provided by FSU 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 FSU is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose, or a fee that is otherwise expressly permitted by other law.

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

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

FSU's policy is that any use or disclosure made pursuant to an authorization may be made only if FSU: (1) determines that the authorization is valid (as described below); (2) verifies the identity of the individual who signed the authorization (see section III.L, "Verifying the Identity of Those Requesting PHI"); and (3) ensures that the use or disclosure is made consistent with the terms of the authorization.

Valid Authorizations. An authorization is valid only if it is written in plain language and contains the following required core elements and statements:

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

- a specific and meaningful description of the PHI to be used or disclosed
- the name or other specific identification of the person or class of persons authorized to use or disclose the PHI
- the name or a description of the person or class of persons to whom FSU may make the requested use or disclosure
- the purpose(s) of the requested use or disclosure. (If the individual initiates the authorization and does not provide a statement of purpose, the statement "at the request of the individual" is sufficient)
- a valid expiration date (e.g., December 31, 2014) or expiration event (e.g., termination from the Health Plan, rejection of an insurance application, etc.)
- the signature of the individual and the date the authorization was signed. (If signed by the individual's personal representative, a description of the representative's authority to act for the individual must also be provided)

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

- a statement of the individual's right to revoke the authorization in writing, and either (1) a list of the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (2) a reference to the Notice of Privacy Practices, if the Notice lists the exceptions to the right to revoke and provides a description of how the individual may revoke the authorization

- a statement informing the individual that:

  FSU may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization; or
  the consequences to the individual if he or she refuses to sign the authorization when:

  - the authorization is to be used to for the Health Plan's eligibility or enrollment determinations or for its underwriting or risk rating determinations, and the authorization is not for the use or disclosure of psychotherapy notes; or

  - a covered entity will be providing health care solely for the purpose of creating PHI for disclosure to a third party and the authorization is to allow the disclosure to the third party (e.g., a physician releasing the results of pre-employment drug testing to FSU)

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

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

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

I. Uses and Disclosures of PHI by Business Associates

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

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

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

- FSU has verified that a valid business associate contract is in place
- the disclosure is consistent with the terms of the business associate agreement
- the disclosure complies with the minimum necessary standard (see section V, "Procedures for Complying with the Minimum Necessary Standard")
- the disclosure is documented in accordance with the Privacy Rules' documentation requirements (see section III.M, "Documentation and Record Retention Requirements"), unless such documentation is unnecessary because the disclosure falls within one of the following categories:
    - payment or health care operations
    - mandatory disclosures of PHI to an individual or to HHS
    - national security and intelligence activities
    - correctional institutions and law enforcement custodians
    - under a valid authorization that is retained as required by the Privacy Rules' documentation requirements (see section III.M, "Documentation Requirements")

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

- the Privacy Officer will immediately notify the business associate in writing of the alleged unauthorized use or disclosure
- the Privacy Officer will telephone the business associate to discuss the alleged unauthorized use or disclosure and to determine whether the unauthorized use or disclosure will cease

- if the business associate does not agree to stop the unauthorized use or disclosure, if FSU learns that the use or disclosure has not stopped, or if the unauthorized use or disclosure is part of a pattern of conduct in violation of the business associate's agreement with FSU, then FSU will:

    - terminate its relationship with the business associate; or

    - if termination is not possible (for example, because there is no other entity in the area that can provide the service), then FSU will report the business associate to the Department of Health and Human Services

- the Privacy Officer will document the known details of the unauthorized use or disclosure for purposes of responding to requests for an accounting of disclosures (see section IV.C)

- if appropriate, the Privacy Officer will follow the procedures set forth in "Mitigation of Inadvertent Disclosures of PHI" (see section III.N)

- the Privacy Officer will follow the Breach Notification Policy contained in section III.N.

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

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

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

- the individual whose PHI is involved has provided a valid authorization allowing disclosure to the spouse, family member or friend, in which case the procedures under the section "Uses and Disclosures of PHI with an Individual's Authorization" must be met (see section III.H)

- the family member is (1) the parent of the individual whose PHI is involved and (2) the individual is a minor child, in which case the procedures under the section "Verifying the Identity of Those Requesting PHI" must be met (see section III.L); or

- the spouse, family member or friend is the personal representative of the individual whose PHI is involved, in which case the procedures under the section "Verifying the Identity of Those Requesting PHI" must be met (see section III.L)

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

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

K. Uses and Disclosures of De-Identified Information

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

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

L. Verifying the Identity of Those Requesting PHI

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

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

- *In Person.* If the individual makes the request in person:

    - request and make a copy of a form of identification from the individual, which may consist of a valid FSU Employee I.D. card, a valid drivers license, a valid passport, or other valid photo identification issued by a government agency

    - verify that the identification matches the identity of the person requesting access to the PHI. If there is any doubt as to the validity or authenticity of the identification, the Privacy Officer must be consulted

    - complete the appropriate sections of FSU's *HIPAA Verification Check List*, including the signature of the person making the inquiry and the date of the inquiry

    - file the *HIPAA Verification Check List*, along with a copy of the identification, in the designated record set of the individual whose records are being accessed in accordance with the Privacy Rules' documentation requirements (see section III.M, "Documentation and Record Retention Requirements")

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

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

- *By E-mail.* If the individual requests PHI through an e-mail request, the receiver is to inform the individual that it is FSU's policy not to provide PHI in response to an e-mail request. The individual should be instructed to make the request in person, or should be directed to send the request in writing using the appropriate form specified in the applicable "Procedures for Complying with Individual Rights" (see section IV)

- *In Writing on the Appropriate Form.* If the individual submits a written request for PHI using the appropriate form:

    - ensure that the form has been completely filled out

    - compare the information in the written request with information in the individual's records. If the information does not match, or if there is any doubt as to the identity of the person making the request, contact the Privacy Officer

- file a copy of the request with the designated record set of the individual whose records are being accessed, in accordance with the documentation requirements (see section III.M, "Documentation and Record Retention Requirements")

- follow the procedures set forth in "Individual's Request to Inspect and Copy" (see section IV.A)

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

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

- verify the identity of the person making the request following the procedures above for responding to a request by an individual

- verify the person's relationship with the child. The relationship may be verified by confirming enrollment of the child as a dependent in the Health Plan

  - generally, a non-custodial parent shall not be denied access to records or information concerning his or her minor child, unless prohibited by court order [discuss with Norbert]

- verify from the Health Plan records that the child is a minor

- verify from the Health Plan records that there is no restriction in place, such as a court order prohibiting release of information to the parent

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

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

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

- verify the identity of the person making the request using the procedures above for responding to a request by an individual
- verify the personal representative's authority to access the individual's record
    - check the individual's file for a copy of a valid power of attorney, order of court, guardianship order, or similar documentation establishing the personal representative's authority. If there is a question as to the scope of authority conferred upon the individual, contact the Privacy Officer to review the document. Advice from legal counsel may also be necessary
    - if the file does not have such documentation
        - obtain a copy of a valid power of attorney, order of court, guardianship order or similar documentation establishing the authority of the personal representative. If there is a question about the validity or sufficiency of the document, or the scope of authority conferred upon the personal representative, contact the Privacy Officer to review the document. Advice from legal counsel may also be necessary.
            - an individual does not have the authority to obtain PHI of his or her spouse without a properly executed authorization from the spouse
        - file a copy of the document in the individual's designated record set according to the documentation requirements (see section III.M)
- follow the appropriate procedures set forth in "Procedures for Complying with Individual Rights" (see section IV)

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

- verify that the request is for one of the purposes set forth above in the sections entitled "Mandatory Disclosures of PHI to Individuals and HHS" (see section III.D) or "Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes" (see section III.E)

- verify that the person is a public official or acting on behalf of a government agency:
    - if the request is made in person:
        - ask to see an agency identification badge, official credentials, or other proof of government status
        - make a copy of the identification provided, write on it the date of the request, and file it with the individual's designated record set
    - if the request is in writing:
        - verify that the request is on appropriate letterhead
        - make a copy of the writing and file it with the individual's designated record set
    - if the request is by a person purporting to act on behalf of a public official:
        - establish that the individual is acting on behalf of the public official, which may be established by one of the following documents:
            - a written statement on appropriate government letterhead that the person is acting under the government's authority
            - a contract for services with the government agency
            - a memorandum of understanding with the government agency
            - a purchase order with the government agency
        - make a copy of the document and file it with the individual's designated record set
    - if there is any question as to the person's identity or affiliation with the government agency, contact the Privacy Officer
- verify that the person is authorized to access the PHI:
    - request a written statement setting forth the legal authority under which the information is being requested

- if under the circumstances a written statement would be impracticable, obtain an oral statement of such legal authority (and document the oral statement)

- if the request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact legal counsel

  - make a copy of the document setting forth the legal authority and file if with the individual's designated record set

- follow the applicable procedures set forth above in the sections entitled "Mandatory Disclosures of PHI to Individuals and HHS" (see section III.D) or "Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes" (see section III.E)

M. Documentation and Record Retention Requirements

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

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

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

FSU's policy is to require proper documentation of uses and disclosures of PHI, as required by the Privacy Rules. The Privacy Officer shall maintain under lock and key the *PHI Disclosure Tracking Forms*. Each form will be maintained for six years beyond the date of the most recent entry on the form. The Privacy Officer will record on the *PHI Disclosure Tracking Forms*, at a minimum, the following information about disclosures of PHI:

- the individual whose PHI FSU is disclosing

- the date of the disclosure

- the name of the entity or person who receives the PHI and, if known, the address of such entity or person

- a brief description of the PHI disclosed

- a brief statement of the purpose of the disclosure

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

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

- in order to avert serious threat to health or safety
- about armed forces personnel to appropriate military command authorities
- for protective services to the President of the United States and other designated persons
- to correctional institutions and law enforcement custodians
- in connection with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault

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

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

Documenting Authorizations and Individual Rights. The Privacy Officer shall maintain under lock and key as part of an individual's designated record set, for a period of six years from the date the document was last effective, the following:

- individual authorizations for the use or disclosure of PHI
- *Requests for an Accounting of Disclosures*, and all accountings and related communications provided in response to the request
- temporary suspensions of an individual's right to an accounting by:
    - a health oversight agency conducting health oversight activities authorized by law, pursuant to 45 CFR 164.512(d)

- a law enforcement official, conducting an activity described in 45 CFR 164.512(f)

- *Requests for Confidential Communications* and all documents relating to their disposition

- *Requests to Inspect and Copy* and all documents relating to their disposition

- *Requests to Amend* and all documents relating to their disposition (if FSU elects to amend PHI, the amendment must be maintained as long as the record is maintained; if FSU elects not to grant the amendment and the individual files a disagreement, the disagreement must be maintained as long as the record is maintained)

- *Requests for Additional Restrictions* and all documents relating to their disposition

- *Individual Complaint Forms*, *Complaint Tracking Forms*, and all other documents relating to their disposition

- an individual's written agreement to receive a Notice of Privacy Practices by e-mail, and any withdrawal of such agreement

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

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

Documenting Disciplinary Action. The Privacy Officer shall maintain under lock and key documentation of all disciplinary action that FSU 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.

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

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

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

N. Mitigation of Inadvertent Disclosures of PHI

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

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

- determine if there are steps that should be taken immediately to prevent any further potential harm to individuals whose PHI is involved in the unauthorized use, and take reasonable and appropriate action to prevent further potential harm, including immediate notification to the Privacy Officer of the unauthorized use or disclosure. The Privacy Officer may consult as necessary with legal counsel

- document the known details of the unauthorized use or disclosure for purposes of responding to a request for an accounting of disclosures (see section IV.C)

- follow any other instructions given by the Privacy Officer to minimize any harm resulting from the use or disclosure

    - if appropriate, follow the Breach Notification Requirements, below

    - evaluate current policies and procedures to determine whether modifications are appropriate

- document all efforts to minimize the harmful effects of the unauthorized use or disclosure in accordance with the Privacy Rules' documentation requirements (see section III.M)

2. Breach Notification Requirements. In the event of a potential breach of protected health information, FSU will investigate the incident. If the incident involves electronic PHI, the investigation will be consistent with FSU's security incident investigation procedures. One or more members of the Breach Notification Team will participate in such investigation, when practical, and report relevant facts to the Team for purposes of determining whether notification will be required. In determining whether notification is required, the Breach Notification Team may consult with any additional employees, agents, contractors or consultants reasonably necessary to determine whether FSU has a duty to notify individuals about a breach.

A. Breach Notification Team

In the event that FSU learns that a breach may have occurred, breach, FSU will establish a Breach Notification Team, which may consists of the following members, as appropriate:

- Privacy Officer
- Security Officer
- FSU legal counsel/outside legal counsel
- Upon request, any individual with knowledge or involvement in the specific incident

B. Determining whether a breach has occurred

When FSU learns of a possible breach, the Breach Notification Team must determine whether there has been an impermissible use or disclosure of unsecured protected health information under HIPAA's Privacy Rule. This includes situations in which a contractor/business associate notifies FSU that an impermissible use or disclosure has or may have occurred. The following are examples of the types of situations that may need evaluation:

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

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

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

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

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

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

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

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

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

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

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 documentation must be retained for a period of at least six years from the date the Team concludes its evaluation of the incident. The Privacy Officer is responsible for retaining the necessary documents.

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

- FSU
- FSU's business associate
- An organized health care arrangement in which FSU 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. FSU or its business associate has a good-faith belief that the unauthorized individual would not reasonably have been able to retain the information.

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

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

Factors to consider include:

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

- What is the likelihood that the information could be re-identified based on the context and the ability to link the information with other available information?

- The unauthorized person who used the information or to whom the disclosure was made?

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

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

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

- Whether the information was actually viewed or acquired?

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

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

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

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

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

C. 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 FSU has a duty to notify FSU of the breach within 60 days, but it is FSU's duty to provide notification to the individuals impacted by the breach. Moreover, if the business associate is considered FSU's agent, FSU 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 FSU of a HIPAA violation, FSU will seek to include in its business associate agreements a provision that requires the business associate to notify FSU within 30 days of discovery. When appropriate, and after reaching consensus with the business associate, FSU may also include a provision in the business associate agreement allocating responsibility for notification between FSU and business associate. When a business associate reports a potential breach to FSU, the Breach Notification Team will work with the business associate to determine whether the incident requires notification.

If the business associate hires any subcontractors, these special requirements should also be included in the business associate's contract with its subcontractors, if applicable.

D. Notification

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

Notice to Individuals. Under HIPAA, FSU must provide notice to affected individuals without unreasonable delay, but no later than 60 days after the date FSU 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, FSU will seek to provide notice as soon as reasonably possible once it has discovered the breach.

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

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach.
- Any steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what FSU 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 FSU knows that an individual is deceased and has the address of the deceased's next of kin or personal representative, FSU may send the written notification to either next of kin or the personal representative.

Under HIPAA, FSU has no more than 60 days after discovery of the disclosure to notify individuals (though disclosure must be made earlier than 60 days if FSU can reasonably do so). The date of discovery is measured as follows:

- First day the breach is known to a member of the FSU's workforce or agents;
    - workforce member includes any employee, partner, volunteer, trainee, agent, etc.
- First day a member of the FSU workforce or its agents **would have known** of the breach by exercising reasonable diligence; or
- First day that FSU 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 FSU does not have sufficient contact information for some or all of the affected individuals (or if the contact information is outdated) then FSU 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 FSU'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 FSU does not have sufficient contact information for the deceased individual's next of kin or personal representative.

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

FSU 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. The Privacy Officer is responsible for retaining these documents.

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

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

Notice to the Department of Health & Human Services. If the Breach Notification Team determines that FSU or its business associate must provide notification to individuals under HIPAA, then FSU 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), FSU will notify the Department of Health & Human Services without unreasonable delay, but no later than 60 days after discovery. This notification is to be submitted to the Department of Health & Human Services contemporaneously with the written notifications sent to individuals and in the manner specified on the Department's Web site.

- If the breach involves fewer than 500 individuals:

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

- The Privacy Officer will submit the log to the Department of Health & Human Services for each calendar year by February 28 of the following year, in the manner specified on the Department's Web site.

Notifications to the Department of Health & Human Services, including the annual log of notifications, must be maintained for at least six years from the date submitted to the Department. The Privacy Officer will retain the necessary documentation.

IV. Procedures for Complying with Individual Rights

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

Information about individuals covered by the Health Plan is found in Health Plan records maintained by FSU and in records maintained by insurers and third party administrators or other business associates involved in the administration of the Health Plan. FSU will respond to individual requests relating to records that it maintains. An individual seeking to exercise his or her individual rights with respect to records held by the Health Plan's insurers or business associates will be directed to submit his or her request directly to the insurer or business associate with the relevant records. If an individual reports that an insurer or third party administrator has not properly handled the request, the HIPAA Compliance Officer will investigate the report under the Complaint procedures (see section II.D, beginning at page 7).

When FSU receives a request for the information that it maintains, FSU will respond to the request using the following procedures.

A. Individual's Request to Inspect and Copy

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

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

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

- the Privacy Rules also allow information to be withheld under the following circumstances, but with a right by the individual to request a review of the decision:
    - a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person
    - the PHI makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that other person
    - the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual
- if there is a question as to whether any restriction or exception applies, contact the Privacy Officer
- no request for access may be denied without the approval of the Privacy Officer

- respond to the request on a timely basis:
    - Privacy Rule response deadlines:
        - if the records are maintained on site, the response is due within 30 days of the request
        - if the records cannot be accessed within the response time:
            - the deadline can be extended 30 days by sending to the individual FSU's *30-Day Extension Letter* explaining the need for an extension of time
            - the letter must be sent within the original 30-day deadline
    - enter response dates into docket or tickler system

- *Requests that Are Denied.* If the request to inspect and copy is denied:
    - the denial must be approved by the Privacy Officer

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

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

        - if the same PHI is maintained in more than one designated record set, or in more than one location, the individual need only be given the information once in response to the request for access

    - the individual has the right to designate a certain form of access (e.g., electronic form, paper form, in person, etc.)

        - if the individual has requested the PHI in a particular format (e.g., electronic file), the information should be provided in that format if it is readily producible in that format

        - otherwise, produce the information in readable hard copy form or in such other form as the individual agrees to receive

        - if the PHI is in coded form, an accurate translation in plain English must be provided

- *Providing a Summary*. Summary or explanation of PHI in lieu of access to record:

    - in lieu of providing access to the record, or in addition to the full record, FSU may provide the individual with a summary or explanation of the information, if the individual:

        - agrees in advance to receive the summary or explanation

        - agrees in advance to pay any fees that may be imposed for the summary or explanation

    - if an individual agrees to accept a summary or explanation and any associated fees:

        - prepare the summary or explanation

        - provide the information in the requested format

- *Charging Reasonable Fees.* FSU may charge the following fees for access to the records:

    - FSU may not charge for retrieving or handling the information

    - if photocopies are requested:

        - FSU may charge for the costs of supplies used in making the copies, including the cost of the paper

        - FSU may charge for the time FSU spent making the copies at the employee's hourly rate. If the employee is a salaried employee, a pro rata hourly rate must be calculated to determine the charge

    - if the information is provided on a computer disk or other portable electronic media, FSU may charge for the cost of the media

    - if the request is to have the records sent by mail or other type of delivery service (such as UPS, Federal Express, etc.), FSU may charge for the actual cost of the postage or delivery service requested

    - if the request is for a summary or explanation of the individual's records, FSU may charge for the time FSU spent preparing the summary or explanation at the employee's hourly rate. If the employee is a salaried employee, a pro rata hourly rate must be calculated to determine the charge

- if the disclosure is made to the parent of a minor or a personal representative, document the disclosure according to the documentation requirements (see section III.M)

- If FSU maintains the information in an electronic form, FSU must be able to provide the information in an electronic form to an individual. FSU 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 FSU cannot provide the information in the requested format, it will offer to produce the information in the formats that are available. If FSU and the individual cannot agree on an electronic format, FSU may produce the records in paper form.

- If an individual's request for access directs FSU to transmit a copy of the information to another person designated by the individual, FSU must provide a copy to the person designated by the individual. The individual's request must be: (1) in writing (2) signed by the individual; (3) clearly identify the designated person; and (4) clearly identify where to send the copy of information. The request does not need to comply with the Authorization requirements.

B. Individual's Request for Amendment

The Privacy Rules give individuals the right to request an amendment of their records that the Health Plan maintains in a designated record set. FSU's policy is that individuals will be given the right to request an amendment of their designated record set as required by the Privacy Rules.

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

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

- the letter must be sent within the original 60-day deadline

- enter response date into docket or tickler system

- *Requests that Are Granted.* If the request for an amendment is approved:

  - send the individual the *Amendment: Grant Letter*

  - make the change in the designated record set. Any records affected must be appended or a link must be provided to the location of the amendment

  - provide notice to the individual and any additional persons or entities listed on the individual's *Request to Amend* form

  - provide notice to any persons/entities known to have the particular record and who may rely on the uncorrected information to the detriment of the individual. Other designated record sets are typically maintained by:

    - third party administrators

- *Requests that Are Denied.* If the request for an amendment is denied, in whole or in part:

  - the denial must be approved by the Privacy Officer

  - the denial must be in writing using FSU's *Amendment: Denial Letter* denying the individual's request for amendment of PHI, setting forth the following information:

    - *The basis for denial.* The appropriate reasons for denying the amendment are:

      - the record or PHI was not created by FSU

      - the record or PHI is not part of the designated record set

      - the record or PHI is not accessible to the individual under the individual's right to inspect and copy

      - the record is already accurate and complete

    - *Explanation of Right to Submit Disagreement.* An explanation of the individual's right to submit a written

statement disagreeing with the denial, with instructions on how to file such a statement

- the written statement shall by submitted on FSU's *Statement of Disagreement Form*
- FSU may prepare a rebuttal to the individual's written statement, which shall be prepared using FSU's *Rebuttal to Statement of Disagreement Form*, a copy of which must be provided to the individual

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

- the individual's record must be updated to reflect the request for amendment and denial:
  - identify the PHI or record that is the subject of the request for amendment
  - append to or otherwise link the PHI or record with the following:
    - the individual's *Request to Amend*
    - FSU's *Amendment: Denial Letter*
    - the individual's *Statement of Disagreement* (if submitted)
    - FSU's *Rebuttal to Statement of Disagreement* (if prepared)
  - all future disclosures of the PHI or record must include the following:
    - if the individual filed a *Statement of Disagreement*, include with the disclosure:
      - the individual *Request to Amend*

- FSU's *Amendment: Denial Letter*
- the individual's *Statement of Disagreement* (if submitted)
- FSU's *Rebuttal to Statement of Disagreement* (if prepared)

- if the individual did not file a *Statement of Disagreement*, include the individual's *Request to Amend* and the *Amendment: Denial Letter* with the record, if the individual has requested such action

- if the PHI or record is being transmitted electronically as part of a standard transaction, FSU may separately transmit the documents noted above to the recipient of the standard transaction

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

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

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

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

- have the individual complete FSU's *Request for an Accounting of Disclosures* form

- verify the identity of the individual (or parent or personal representative) using the procedures set forth above under "Verifying the Identity of Those Requesting PHI" (see section III.L)

- record the request on the *Disclosures Requests Tracking Form*

- determine whether the individual has previously requested an accounting

- the Privacy Rules require FSU to provide one accounting to an individual in any 12 month period without a charge. FSU's policy is to provide two accountings to an individual in any 12 month period without a charge

- if the individual has made two requests within the 12 months prior to the date of the current request:

  - FSU may charge for its actual costs in responding to the request

    - the charge may not include a charge for retrieving or handling the information

    - FSU may charge for the time FSU spends preparing the accounting at the employee's hourly rate. If the employee is a salaried employee, a pro rata hourly rate must be calculated to determine the charge

  - provide individual with the *Accounting of Disclosures Letter* informing him or her:

    - the fee that will be charged for the additional accounting

    - that the individual may withdraw or modify the request in order to avoid or reduce the fee

- determine whether there has been a temporary suspension imposed on the individual's right to an accounting

  - a health oversight agency or law enforcement official, in appropriate circumstances, may suspend an individual's right to an accounting if the accounting would impede the agency's activities

  - if a suspension has been documented, contact the Privacy Officer for guidance

- respond to the request for an accounting on a timely basis:

  - a written response is due within 60 days that either:

    - provides the accounting; or

    - informs the individual that there have been no disclosures that must be included in the accounting

- enter response dates into docket or tickler system
- if the accounting cannot be provided within 60 days:
  - the deadline can be extended 30 days by sending to the individual FSU's *30-Day Extension Letter* explaining the need for an extension of time
  - the letter must be sent within the original 60-day deadline

- in preparing the accounting, include disclosures following these guidelines:
  - include all disclosures (but not uses) of the requesting individual's PHI made by the Health Plan and any of its business associates during the period six years prior to the date of the request
  - the accounting does not have to include disclosures made:
    - to carry out treatment, payment or health care operations
    - to the individual who is the subject of the PHI
    - incident to an otherwise permitted use or disclosure
    - pursuant to the individual's authorization
    - for specific national security or intelligence purposes
    - to correctional institutions or law enforcement custodians when the disclosure was permitted without an authorization
    - as part of a limited data set
- determine whether accounting information must be obtained from business associates
  - review contracts with business associates to determine which business associates have authority to disclose the individual's PHI
  - contact business associates with authority to disclose PHI to request the information necessary to respond to the accounting
    - follow contractual provisions for providing notice to business associate of individual's request for accounting
    - pursue contacts by phone to monitor the status of business associates' response to the request

- for each reportable disclosure, provide the following information:
    - the date of the disclosure
    - the name and, if known, the address of the entity or person who received the PHI
    - a brief description of the PHI disclosed
    - the reason for the disclosure, which may be in the form of:
        - a brief statement of the reason for the disclosure that reasonably informs the individual of the basis for the disclosure; or
        - if applicable, a copy of a written request for the disclosure when the disclosure was:
            - in response to a request from HHS
            - one of the permitted disclosures of PHI for legal and public policy purposes
    - if during the accounting time period FSU has made multiple disclosures of the individual's PHI to the same person or entity for a single purpose, these multiple disclosures may be accounted for as follows:
        - for the first disclosure, provide all of the details listed above
        - for the subsequent disclosures, provide:
            - the frequency, periodicity, or number of disclosures made during the accounting period; and
            - the date of the last such disclosure during the accounting period
- document the disclosure according to the Privacy Rules' documentation requirements (see section III.M).

D. Individual's Request for Confidential Communications

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

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

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

        - inform the individual whether the request is being granted or not

    - if the request does not indicate that disclosure of all or part of the information to which the request pertains could endanger the individual:

        - it is FSU's policy to accommodate the request whenever reasonable. FSU will consider the nature of the request and the difficulty of complying with the request

        - if the individual's request, as stated, cannot be accommodated, the individual should be contacted in person, in writing, or by telephone to explain why the request cannot be accommodated and to determine if an alternate arrangement for confidential communications can be worked out

        - if anything is unclear about the instructions for confidential communications, the individual should be promptly contacted in order to clarify the instructions

        - notify the individual to indicate whether the request is being granted or not

- if a request for confidential communications is approved:

    - promptly update the information in the individual's benefit file to indicate that confidential communications must be delivered by the designated alternate means

    - promptly update the individual's contact information on FSU's electronic data system to indicate that communications to the individual must be delivered by the designated alternate means

    - promptly notify and convey to any relevant third party administrator(s) the request for alternative communications with instructions for the third party administrator(s) to update their records

    - promptly notify and convey the request to any other third parties known to maintain records and communicate with the individual the request for confidential communications

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

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

The Privacy Rules give individuals their right to request that FSU restrict its uses or disclosures of their PHI beyond the restrictions imposed by the Privacy Rules. The Privacy Rules do not require FSU to agree to any requested restrictions. FSU's policy is to permit an individual to request restrictions on uses and disclosures as required by the Privacy Rules.

FSU shall respond to a request for restrictions on uses and disclosures of PHI by an individual, a parent of a minor child, or a personal representative using the following procedures:

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

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

V. Procedures for Complying with the Minimum Necessary Standard

The Privacy Rules require that, for most purposes, FSU limit its uses and disclosures to the minimum necessary to accomplish the purpose of the use or disclosure. When possible, the minimum amount of information necessary should be "Limited Data Set" information (see the section "Important Definitions and Concepts Used in these Policies and Procedures"). When additional information is needed, FSU will use and disclose only the addition information needed for the specific purpose. FSU's policy is to limit uses and disclosures to the minimum necessary, unless an exception applies. When a use or disclosure is done on a routine basis, the procedures for that use or disclosure (contained below) will reflect FSU's minimum necessary policy. When a use or disclosure is not a routine function, the use or disclosure must be evaluated by the Privacy Officer to ensure that it complies with the minimum necessary standard.

A. <u>Determining the Minimum Necessary – Use and Disclosure Criteria</u>

If more information is needed beyond Limited Data Set information, the following criteria should be taken into account for evaluating whether a use or disclosure is limited to the minimum necessary to accomplish the intended purposes:

- the type of PHI needed
- for uses and disclosures within FSU, whether they are to the persons or class of persons who need access to the information to carry out their job duties in connection with the Health Plan
- whether the use is for treatment, payment or health care operations, or is made pursuant to a valid authorization by the individual, or otherwise allowed under the Privacy Rules
- whether the task can be accomplished with less information
- whether, under the circumstances, the use or disclosure seems to be reasonably necessary and appropriate
- the risk that the use or disclosure will result in an unauthorized use or disclosure of the PHI
- if the disclosure will be to a business associate, whether FSU has entered into a valid business associate agreement with that business associate
- if the disclosure will be to a third party, whether it is reasonable under the circumstances to rely upon the judgment of the party requesting the

disclosure. Privacy Rules permit such reliance when the request is made by:

  - a public official or agency for a permitted disclosure of PHI for legal or public policy purposes
  - another covered entity
  - a professional who is a workforce member or business associate of the covered entity holding the information
  - a researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board

- whether FSU has agreed to an additional restriction on the use or disclosure of PHI that would be violated by the use or disclosure
- other additional criteria the Privacy Officer should consider under the circumstances

B. Routine and Non-routine Uses and Disclosures of PHI

The following uses and disclosures of PHI are *routine uses and disclosures* for which FSU has established procedures that are to be followed to ensure compliance with the minimum necessary standard:

- assisting new hires (or existing employees who have not previously enrolled) with Health Plan enrollment paperwork
- processing Health Plan enrollment or disenrollment paperwork
- processing change of status information for Health Plan participants
- reporting enrollment, disenrollment and change of status information to the Plan's insurer or third-party administrator
- responding to employee questions regarding coverage and payment under the Health Plan
- updating FSU's Health Plan information system with eligibility, coverage, and payment information
- responding to claims appeals under the Health Plan
- submitting claims to reinsurers, including stop-loss insurance carriers and excess loss insurance carriers

- reviewing Health Plan performance

All *non-routine uses or disclosures* must be approved by the Privacy Officer to ensure that they comply with the minimum necessary standard.

C. Routine and Non-routine Requests

The following requests for PHI are *routine requests* for which FSU has established procedures that are to be followed to ensure compliance with the minimum necessary standard:

- requests from health care providers to confirm insurance coverage
- requests from other insurers for purposes of coordinating benefits
- requests from Friend of the Court to document that benefits are being provided to an individual
- requests from state or federal social service agencies
- requests involving qualified medical child support orders

All *non-routine requests* must be approved by the Privacy Officer to ensure that they comply with the minimum necessary standard. Please note the following:

- in Michigan, if confidential mental health information is disclosed, the identity of the individual to whom it pertains must be protected

D. Exceptions to the Minimum Necessary Standard

The minimum necessary standard does not apply to:

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

- disclosures pursuant to process or as otherwise required by law
- uses or disclosures that are required for compliance with the Privacy Rules