FERRIS STATE UNIVERSITY

HIPAA Breach Notification Policy

1. Security Incident Response Advisory Team.

Ferris State University ("Ferris State"), a hybrid entity with health care components, has established a Security Incident Response Advisory Team (SIRAT), which consists of the following members:

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

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

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

2. Investigation

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

Upon notification of a potential incident of unauthorized access to PHI, the Privacy Officer of the health care component where the violation may have occurred will determine whether Ferris State has a duty to notify individuals about a breach. In determining whether notification is required, the Privacy Officer of the health care

component where the violation may have occurred may consult with legal counsel, employees, agents, contractors or consultants as reasonably necessary to determine Ferris State's notification obligations, if any.

3. Determine whether a breach has occurred.

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

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

If a situation requires evaluation, the Security Incident Response Advisory Team should gather details about the incident, including the following:

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

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

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

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

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

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

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

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

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

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

        - For data in motion (which includes data moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange), the encryption

process must comply, as appropriate, with one of the following:

- National Institute of Standards & Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*;

- National Institute of Standards & Technology Special Publication 800-77, *Guide to IPsec VPNs;*

- National Institute of Standards & Technology Special Publication 800-113, *Guide to SSL VPNs*; or

- Other encryption processes that are Federal Information Processing Standards 140-2 validated.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    a. The disclosure is made to an unauthorized individual.

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

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

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

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

Factors to consider include:

- The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification.
    - Did it include social security numbers, driver's license numbers, bank account/credit card numbers, insurance numbers, or other sensitive information that could be used for identity theft or identity fraud crimes?
    - Did it include information about medical treatment, diagnoses, diseases, or similar details about an individual's health?
    - What is the likelihood that the Protected Health Information could be reidentified based on the context and the ability to link the information with other available information?
- The unauthorized person who used the Protected Health Information or to whom the disclosure was made.
    - Was the recipient also a HIPAA covered entity with a legal duty not to misuse the information?
    - Does the recipient have a contractual relationship with Ferris State that prohibits it from misusing the information?
    - Are there other facts and circumstances that would indicate that the recipient of the information is unlikely to misuse the information?

- Whether the Protected Health Information was actually acquired or viewed.
    - Does a forensic analysis indicate that Protected Health Information on a lost computer was never accessed, viewed, acquired, transferred or otherwise compromised??
- The extent to which the risk to the PHI has been mitigated.
    - Are there past dealings with the recipient or other factors that would indicate that the recipient can be trusted not to use or further disclose the information?

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

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

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

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

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

5. Notification

If the Security Incident Response Advisory Team determines that Ferris State must provide notification of the incident, the Team will prepare appropriate notification as required below.

A. Notice to Individuals

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

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

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

All notifications must be written in plain language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Notice to the Media

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

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

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

C. To the Department of Health & Human Services

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

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

- If the breach involves fewer than 500 individuals:

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

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

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

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

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

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

- Ferris State will notify the covered entity as soon as possible after discovering a potential breach, and no later than 60 days after discovery.
- Ferris State will provide the covered entity with the following information, either at the time Ferris State provides notice of the potential breach to the covered entity or promptly thereafter as the information becomes available:
    - The identity of each individual whose unsecured protected health information has been, or is reasonably believed to have been, breached, to the extent possible.
    - Any other available information that the covered entity is required to include in the notification to the individual. This may include the following:
        - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
        - A description of the types of unsecured protected health information that were involved in the breach.
        - Any steps the individual should take to protect themselves from potential harm resulting from the breach.
        - A brief description of what Ferris State is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
        - Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.

- Ferris State will cooperate with covered entity in determining whether notification is required under HIPAA.