ADMINISTRATIVE REGULATION AND PROCEDURE

Title: REPORTABLE BREACH NOTIFICATION	Code: CC0901 Revised: 09/25/17
Policy Reference: C0900 and E0202	

I. Introduction

This Reportable Breach Notification Procedure is adopted by Milwaukee Area Technical College and any group health insurance plan sponsored by Milwaukee Area Technical College (collectively "MATC or the college"), as part of the Plan's Privacy Procedure (CC0900). This Procedure is intended to comply with the final HITECH regulations at 45 CFR §164.400 et seq. for breaches occurring on or after September 23, 2013 ("HIPAA Breach Regulations"), as well as Wis. Stats. § 134.98, the Family Education Rights and Privacy Act ("FERPA") and any other law or regulation applicable to MATC which protects privacy of information and/or requires data breach notification.

Under the HIPAA Breach Regulations, if a Reportable Breach of unsecured protected health information has occurred, the Plan must comply with certain notice requirements with respect to the affected individuals, HHS, and, in certain instances, the media. Under Wis. Stat. § 134.98, covered entities are required to provide notice of breach in certain circumstances where personal identifying information is compromised. For purposes of administration, MATC will use the Reportable Breach standards set forth in the HIPAA amendments to govern its response, in situations involving Protected Health Information (PHI) under HIPAA, as well as Personally Identifiable Information (PII) under FERPA, and any privacy protected personal identifying information under state or federal law.

MATC's Privacy Official is the Assistant General Counsel. MATC's Security Official is the Manager of Information Security. The Security Official is responsible for the development and implementation of security controls, technical controls and access limitations relating to security of MATC systems on which PHI or PII may be stored.

II. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply and MATC will not provide notice.

The Privacy Official is responsible for reviewing the circumstances of possible breaches brought to his or her attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Procedure and the Breach Regulations. All Business Associates under contract with MATC, and all workforce members who have access to PHI, PII and private information, are required to report to the Privacy Official any incidents involving possible breaches.

Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the privacy rules is presumed to be a Reportable Breach, unless the Privacy Official determines that there is a low probability that the privacy or security of the protected health information has been or will be compromised. Unauthorized access, use or disclosure of PII or privacy protected education records and other data will be analyzed using the same methodology.

Attachment of ransomware or similar malware to MATC network systems that contain PHI will be considered a reportable incident, to which MATC's breach response protocol will apply. In the event of ransomware detection, the Privacy Official will seek to impose interception technology and notification systems if possible. In the event that ransomware is intercepted and PHI has not been compromised, an incident of ransomware may be considered less than a Reportable Breach.

The Privacy Official's determination of whether a Reportable Breach has occurred must include the following considerations:

- Was there a violation of HIPAA Privacy Rules, FERPA or other privacy protection law or regulation? There must be an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA Privacy Rules by the Plan or a Business Associate of the Plan in order for a situation to rise to the level of Reportable Breach under HIPAA. Likewise, there must be a violation of FERPA, or other privacy protection law or regulation to give rise to a Reportable Breach. If not, then the notice requirements do not apply.

- Was protected health information (PHI) personal identifying information (PII) or privacy protected data involved? If not, then the notice requirements do not apply.

- Was the protected information secured? For electronic protected health information to be "secured," it must have been encrypted to NIST standards or destroyed. Education records and other privacy protected personal identifying information is secure if encrypted. For paper protected data to be "secured," it must have been destroyed. If yes, then the notice requirements do not apply.

- Was there unauthorized access, use, acquisition, or disclosure of protected information? To be reportable, based upon the totality of information known to the Privacy Official, there must be evidence of unauthorized use, unauthorized acquisition or unauthorized disclosure of a category of protected information, such as PHI.

- Is there a low probability that privacy or security was compromised? If the Privacy

Official determines that there is only a low probability of compromise, then the notice requirements do not apply. To determine whether there is only a low probability that the privacy or security of the protected health information was compromised, the Privacy Official must perform a risk assessment that considers at least the following factors:

- The nature and extent of the protected information involved, including the types of identifiers and the likelihood of re-identification. For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud; did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual or otherwise to further the unauthorized recipient's own interests.

- The unauthorized person who used the protected information or to whom the disclosure was made. For example, does the unauthorized recipient of the protected health information have obligations to protect the privacy and security of the protected health information, such as another entity subject to the HIPAA privacy and security rules or an entity required to comply with the Privacy Act of 1974 or the Federal Information Security Management Act of 2002, and would those obligations lower the probability that the recipient would use or further disclose the protected health information inappropriately? Also, was the protected health information impermissibly used within a covered entity or business associate, or was it disclosed outside a covered entity or business associate?

- Whether the protected information was actually acquired or viewed. If there was only an opportunity to actually view the information, but the Privacy Official determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer with was lost or stolen and subsequently recovered, and the Privacy Official is able to determine (based on a forensic examination of the computer) that none of the information was actually viewed, there may be no probability of compromise.

- The extent to which the risk to the protected information has been mitigated. For example, if MATC can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient of that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

If the Privacy Official determines that there is only a low probability that the privacy or security of the information was compromised, then the Plan will document the determination in writing, keep the documentation on file, and not provide notifications. On the other hand, if the Privacy Official is not able to determine that there is only a low probability that the privacy or security of the information was compromised, the Plan will provide notifications.

Exceptions to Notification Requirement

If an exception applies, then a Reportable Breach has not occurred, and the notice requirements are not applicable. For purposes of administration, MATC will treat the following HIPAA privacy rule exceptions as exceptions under other privacy protection laws and regulations, including state law.

Exception 1: A Reportable Breach does not occur if the breach involved an unintentional access, use, or acquisition of protected health information by a workforce member or Business Associate, if the unauthorized access, use, acquisition, or disclosure-(a) was in good faith; (b) was within the scope of authority of the workforce member or Business Associate; and (c) does not involve further use or disclosure in violation of the HIPAA privacy rules.

Exception 2: A Reportable Breach has not occurred if the breach involved an inadvertent disclosure from one person authorized to have access to protected information to another person at the same covered entity or Business Associate also authorized to have access to the protected health information, provided that there is no further use or disclosure in violation of the HIPAA privacy rules.

Exception 3: A Reportable Breach has not occurred if the breach involved a disclosure where there is a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the protected information.

Maintenance of Breach Documentation. The Plan shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of individuals affected. This includes any incident involving ransomware, malware or other security breaches wherein security of PHI may be compromised. The following information should be documented for each breach and stored in the General Counsel files:

a. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of health plan participants affected, if known.

b. A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
c. A description of the action taken with regard to notification of affected plan participants regarding the breach.

d. Steps taken to mitigate the breach and prevent future occurrences.

Breach incident documentation may be shared with the Plan's legal counsel, insurance carrier or law enforcement.

III. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If the Privacy Official determines that a Reportable Breach has occurred, the Privacy Official will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. MATC has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce members are trained to notify the Privacy Official or other responsible person immediately so the college (and its covered health plans) can act within the applicable time periods.

The Privacy Official is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Official may, on behalf of the Plan, engage a third party (including a Business Associate) to assist with preparation and delivery of any required notices.

The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the college had actual knowledge of the breach. The Privacy Official will determine the date of discovery as the earlier of-(1) the date that a workforce member (other than a workforce member who committed the breach) knows of the events giving rise to the breach; and (2) the date that a workforce member or agent of the college, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence.

Except as otherwise specified in the notice sections that follow, notices must be given "without unreasonable delay" and in no event later than 60 calendar days after the discovery date of the breach. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not impede the notice deadline.
Time limits will be extended in the event a law enforcement official requests that the

college delay giving notices.

IV. Business Associates

If a Business Associate of MATC commits or identifies a possible Reportable Breach relating to participants in an MATC-sponsored employee benefit plan, the Business Associate must give notice to MATC. MATC is responsible for providing any required notices of a Reportable Breach to individuals, HHS, and (if necessary) the media. Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Plan's notice obligations is the date that the Plan receives notice from the Business Associate.

In its Business Associate contracts, the Plan will require Business Associates to:

- report incidents involving breaches or possible breaches to the Privacy Official in a timely manner;

  provide to the college any and all information requested by the college regarding the breach or possible breach, including, but not limited to, the information required to be included in notices (as described below); and

- establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

V. Notice to Individuals

In the event of a Reportable Breach, notice will be given to individuals without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

A. Content of Notice to Individuals

Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- A brief description of the incident.

- If known, the date of the Reportable Breach and the Discovery Date.
  A description of the types of unsecured protected information involved in the Reportable Breach (for example, full name, Social Security numbers, address, diagnosis, date of birth, account number, disability code, or other).
  The steps individuals should take to protect themselves (such as contacting credit

card companies and credit monitoring services).

- A description of what the college is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.
- A description of what the college is doing to mitigate harm to individuals.
- A description of what measures the college is taking to protect against further breaches (such as sanctions imposed on workforce members involved in the Reportable Breach, encryption, installation of new firewalls).
- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

B. Types of Notice to Individuals

MATC will deliver individual notices using the following methods, depending on the circumstances of the breach and the college's contact information for affected individuals.

Actual Notice will be given in all cases, unless MATC has insufficient or out-of-date addresses for the affected individuals. Actual written notice:

- will be sent via first-class mail to last known address of the individual(s);
- may be sent via email instead, if the individual has agreed to receive electronic notices;
- will be sent to the parent on behalf of a minor child; and
- will be sent to the next-of-kin or personal representative of a deceased person, if the college knows the individual is deceased and has the address of the next-of-kin or personal representative.

Substitute Notice will be given if MATC has insufficient or out-of-date addresses for the affected individuals.

- If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, an alternate written notice, or other means.

- If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.

  Substitute notice via website. Conspicuous posting on home page of the MATC website for 90 days, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. Contents of the notice can be provided directly on the website or via hyperlink.
  Substitute notice via media. Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. It may be necessary to give the substitute notice in both local media outlet(s) and statewide media outlet(s) and in more than one state.

  Substitute Notice is not required if the individual is deceased and MATC has insufficient or out-of-date information that precludes written notice to the next-of-kin or personal representative of the individual.

Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured protected information may occur. Urgent notice must be given by telephone or other appropriate means.

VI. Notice to HHS – PHI Breach Only

In situations governed by HIPAA involving breach of protected health information specifically notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

Immediate Notice to HHS. If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

Annual Report to HHS. The Privacy Official will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals, and will report to HHS the Reportable Breaches that were discovered in the preceding calendar year. The reports are due within 60 days after the end of the calendar year. The reports will be submitted as directed on the HHS website.

VII. Notice to Media (Press Release) – PHI Breach Only

In situations governed by HIPAA involving Reportable Breach of personal health information, notice to media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 residents of any one state or jurisdiction. If notice to media is required, notice will be given to prominent media outlets serving the state or jurisdiction.

If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for giving notice to the media.

VIII. Complaints

MATC's Assistant General Counsel will be the Plan's contact person for receiving complaints. Complaints should be directed to Office of General Counsel, Room M-278, 700 W. State St., Milwaukee, WI 53233; 414-297-7307; fax 414-297-6484.
The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

Maintenance of Breach Documentation. The Plan shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of individuals affected. This includes any incident involving ransomware, malware or other security breaches wherein security of PHI may be compromised. The following information should be documented for each breach and stored in the General Counsel files:

a. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of health plan participants affected, if known.
b. A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
e. A description of the action taken with regard to notification of affected plan participants regarding the breach.

f. Steps taken to mitigate the breach and prevent future occurrences.

Breach incident documentation may be shared with the Plan's legal counsel, insurance

carrier or law enforcement.