UNIVERSITY OF MAINE SYSTEM
HIPAA POLICY #8
NOTIFICATION OF BREACH

I. Introduction

HIPAA requires covered entities (CEs) to provide notification to affected individuals and to the Secretary following the discovery of a breach of unsecured protected health information (PHI.) In addition, in some cases, HIPAA requires CEs to provide notification to the media of breaches. In the case of a breach of unsecured PHI at or by a business associate (BA) of a CE, HIPAA requires the BA to notify the CE of the breach.

In addition to the breach notification provisions for HIPAA CEs and BAs, the Federal Trade Commission (FTC) imposes similar breach notification requirements upon vendors of personal health records (PHRs) and their third party service providers following the discovery of a breach of security of unsecured PHR identifiable health information.

II. Definition of Breach

Health Care Components and Business Associate Components of the University of Maine System shall take the following steps to determine whether a breach requiring notification has occurred. First, they must determine whether there has been an impermissible acquisition, access, use or disclosure of PHI under the Privacy Rule. Second, they must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the PHI. Lastly, they need to determine whether the incident falls under one of the exceptions to the definition of "breach."

Breach" does not include:

(i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or a BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

(iii) A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Apart from the exceptions listed above, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is <u>presumed</u> to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated.

III. Unsecured PHI

Covered Components that implement specified technologies and methodologies with respect to PHI are <u>not</u> required to provide notifications in the event of a breach of such information because the information is not considered "unsecured" in such cases. **Unsecured PHI** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. <u>Encryption</u> and <u>destruction</u> are the only two technologies and methodologies specified by the Secretary for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

IV. Notification of Breach

A. Notification to Individuals

A Health Care Component shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the Health Care Component to have been, accessed, acquired, used, or disclosed as a result of such breach.

A Health Care Component shall provide the required notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. A breach shall be treated as discovered as of the first day on which such breach is known, or, by exercising reasonable diligence would have been known, to the Health Care Component. A Health Care Component shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Health Care Component.

The required notification shall be written in plain language and shall include, to the extent possible:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(4) A brief description of what the Health Care Component is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

The required notification to individuals shall be provided in the following form:

(1) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(2) If the Health Care Component knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(3) In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual. Substitute notice must consist of all of the following:

(i) E-mail notice, if the person has e-mail addresses for the individuals to be notified;

(ii) Conspicuous posting of the notice on the home page of the Web site of the Health Care Component;

(iii) Notification to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(iv) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

(4) In any case deemed by the Health Care Component to require urgency because of possible imminent misuse of unsecured PHI, the Health Care Component may provide information to individuals by telephone or other means, as appropriate, in addition to the other forms of

notice.

B. Notification to the Media

For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, the Health Care Component shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. The Health Care Component shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The required notification shall be written in plain language and shall include, to the extent possible:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(4) A brief description of what the Health Care Component is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

C. Notification to the Secretary

A Health Care Component shall, following the discovery of a breach of unsecured PHI, notify the Secretary.

For breaches of unsecured PHI involving 500 or more individuals, the Health Care Component shall provide notification to the Secretary contemporaneously with the notice provided to individuals and in the manner specified on the HHS Web site.

For breaches of unsecured PHI involving less than 500 individuals, the Health Care Component shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification to the Secretary for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

D. Notification by a Business Associate Component

A Business Associate Component shall, following the discovery of a breach of unsecured PHI, notify the Covered Entity of such breach. A breach shall be treated as discovered by a Business Associate Component as of the first day on which such breach is known or, by exercising reasonable diligence, would have been known to the Business Associate Component. A Business Associate Component shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the Business Associate Component.

A Business Associate Component shall provide the required notification immediately and in no case later than 60 calendar days after discovery of a breach. The notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. The Business Associate Component shall provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual as information becomes available.

E. Law Enforcement Delay

If a law enforcement official states to a Health Care Component or Business Associate Component that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, a Health Care Component or Business Associate Component shall:

(1) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(2) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (1) is submitted during that time.

F. Notification to Consumer Reporting Agencies

If a Health Care Component discovers a breach of security of electronic PHI that requires notification to more than 1,000 persons at a single time, the HCC shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

G. Notification to State Regulators

When notice of a breach of security of electronic PHI is required, the Health Care Component shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the HCC is not regulated by the Department, the Attorney General.

Revised 05/10/2013