Section 1: GENERAL PRIVACY RULES

1.8 Breach Notification for Privacy Violations, Appendix A: HIPAA

POLICY

1. Breach Response: The University of Florida (UF) uses and discloses protected health information (PHI) in its role as a Covered Entity (CE). Reports and discoveries of breaches of "unsecured" PHI (see definition below) will be investigated to determine:
    a. Whether unsecured PHI has been, or is reasonably believed by UF to have been accessed, acquired, or disclosed as a result of such breach; and
    b. The degree to which the security or privacy of the PHI may have been compromised.
2. Assessment for Low Probability of Compromise: If an assessment of a confirmed breach of unsecured PHI indicates that there was not a low probability that the security or privacy of the PHI was compromised, UF will make reasonable efforts to notify each affected individual of the breach within 60 days, as required by the Breach Notification Rule.
3. The Privacy Office shall:
    a. Receive privacy-related complaints or incidents by telephone, email, fax, or mail.
    b. Register each alleged privacy violation in the online registration/tracking system, which will automatically generate a case-number.
    c. Retain all related documents into the system under the appropriate case-number.
    d. Add notes and other documentation as needed throughout the investigation.

DEFINITIONS

1. ***Breach (HIPAA)***: A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI or personal information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment. Exceptions apply.
    a. Breach <u>does not</u> 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 business associate (BA) if such acquisition, access, or use was made in good faith and within the course and 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.

b. Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy and Security Rules is presumed to be a breach unless the CE or BA, 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:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

2. ***Notification:*** The act of informing persons affected by a breach of private information that their information was included and steps they can take to protect themselves and their privacy.
3. ***Privacy Complaint***: An allegation by an individual that an organization is not complying with the requirements of the federal privacy and/or security regulations or the organization's own policies and procedures related to the privacy / security of personal information.
4. ***Privacy Incident:*** A known or suspected action, inconsistent with the organization's privacy policies and procedures, or an adverse event, related to PHI.
5. ***Unsecured Protected Health Information***: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary (of Health and Human Services); specifically, encryption for electronic PHI, and destruction for all other PHI.

PRIVACY REQUIREMENTS

1. Notification to Individuals Required: A CE shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been accessed, acquired, used, or disclosed as a result of such breach.
   a. Breaches treated as discovered: For purposes of paragraph (1) above, a breach shall be treated as discovered by a CE as of the first day on which such breach is known to the CE, or, by exercising reasonable diligence would have been known. A CE 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 CE (determined in accordance with the federal common law of agency).
   b. Timeliness of notification: Except as provided in § 164.412 (see Law Enforcement Delay below), a CE shall provide the required notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
   c. Content of notification: The required notification shall be written in plain language and shall include, to the extent possible:
      i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
      ii. 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);
      iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. A brief description of what the CE involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
v. 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.

d. Methods of individual notification: The notification shall be provided in the following forms:

i. Written notice. The notification may be provided in one or more mailings as information is available.

- 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.
- Written notification by first class mail to either the next of kin or personal representative of a deceased individual.

ii. Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual or to the next of kin or personal representative of a deceased individual, a substitute form of notice reasonably calculated to reach the individual shall be provided.

- For fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.
- For 10 or more individuals, substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the CE involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and 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.

iii. Additional notice in urgent situations. In any case deemed by the CE to require urgency because of possible imminent misuse of unsecured PHI, the CE may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph 1) above.

2. Notification to the media

a. For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, a CE shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. The content of the notice shall meet the same requirements as the written notification to individuals described above.

b. Timeliness of notification. Except as provided in § 164.412 (see Law Enforcement Delay below), a CE shall provide the notification required by paragraph a. without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

3. Notification to the Secretary: A CE shall, following the discovery of a breach of unsecured PHI, notify the Secretary.

a. For breaches involving 500 or more individuals, a CE shall, except as provided in §164.412 (see Law Enforcement Delay below), provide the notification contemporaneously with the written notice to affected individuals and in the manner specified on the HHS Web site.

b. For breaches involving less than 500 individuals, a CE 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 for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

4. Notification by a Business Associate

   a. General rule: A BA shall, following the discovery of a breach of unsecured PHI, notify the CE of such breach.

   b. Breaches treated as discovered: For purposes of the above paragraph, a breach shall be treated as discovered by a BA using the same guidelines specified above.

   c. Timeliness of notification: Except as provided in § 164.412 (see Law Enforcement Delay below), a BA shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

   d. Content of notification: To the extent possible, the BA should provide the CE with the identification of each individual affected by the breach as well as any information required to be provided by the CE in its notification to affected individuals.

5. Law enforcement delay (§ 164.412)

   a. If a law enforcement official states to a CE or BA that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a CE or BA shall:

      i. 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

      ii. 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 above is submitted during that time.

6. Burden of proof: In the event of a use or disclosure in violation of the Privacy Rule, the CE or BA, as applicable, shall have the burden of demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach, as defined in the HIPAA Requirements.

REFERENCES

1. HIPAA Regulations: 45 CFR §160.306 Complaints to the Secretary; §164.400 – 414 Notification in the Case of Breach of Unsecured Protected Health Information; §164.530(d) Complaints, (e) Sanctions, and (f) Mitigation
2. UF Regulations: 1.013 Policies on Restricted Data

EXHIBITS

None