Privacy Incident Response and Breach Notification Procedures

Procedures

1. UNMC shall immediately respond to privacy incidents to ensure confidentiality is maintained and to mitigate any adverse effects resulting from the incident. Individuals and the U.S. Department of Health and Human Services shall be notified following the discovery of breach of unsecured protected health information (PHI) as required by the Health Insurance Portability and Accountability Act.

   a. Suspected patient-related privacy incidents shall be reported in accordance with:

      i. UNMC Policy No. 6057, Use and Disclosure of Protected Health Information and related procedures
      ii. UNMC Policy No. 6062, Patient/Consumer Complaints
      iii. UNMC Policy No. 6045, Privacy, Confidentiality and Information Security, and related procedures
      iv. Other UNMC policies and procedures governing protected health information as applicable.

2. Suspected privacy incidents shall be reported to the Privacy Office immediately for further investigation.

3. Notification of Breach of Unsecured PHI. The Privacy Office shall notify individuals and the U.S. Dept or Health and Human Services of breaches of unsecured PHI in writing as required by HIPAA at 45 CFR 164.400-414)

   a. Workforce members and business associates shall immediately notify the Privacy Office of any suspected impermissible use or disclosure of PHI. The Privacy office will investigate all reports of suspected breaches of PHI to determine if the incident violates the Privacy Rule.

   b. If a Privacy rule violation has occurred, the Privacy office will conduct a documented risk assessment to determine if there is a significant risk of financial, reputational, or other harm to the individual(s) affected. Consideration of who impermissibly used/to whom the information was impermissibly disclosed will be documented, as well as the type and amount of PHI involved in the impermissible use or disclosure.

   c. Exceptions. If a significant risk of financial, reputational or other harm to the individual(s) may have occurred, the Privacy Office will determine and document if the violation falls within any of the following three exceptions to the Breach Notification rule:

      i. Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of the ACE or a business associate of the ACE without further impermissible use or disclosure (i.e. accidently accessing the wrong patient in the medical information system because the wrong medical record number or name was used by mistake).

      ii. Inadvertent disclosure of PHI from one person authorized to access PHI at the ACE or a business associate of the ACE to another person authorized to access PHI at the ACE or business associate without further impermissible use or disclosure (i.e. misdirected interoffice mail containing PHI)

      iii. Unauthorized disclosure in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information (i.e. Test results or bills are sent to the wrong individuals, but are returned by the post office unopened as undeliverable)

   d. Notification. If the privacy violation involving significant risk of financial, reputational or other harm to the individual does not fall within one of the regulatory exceptions listed above, the Privacy Office will notify the affected individual(s) in writing without unreasonable delay, but within 60 calendar days after the date the breach was discovered by the ACE or the date the business associate notified the ACE of the breach.
i. The Privacy office shall send letters to individuals by first-class mail to their last known address. For deceased individuals, the letter will be sent to the last known address of the listed next-of-kin.

ii. **Content.** The notification will contain: a description of what happened, the types of unsecured PHI involved, any steps the individual should take to protect themselves from harm, what the ACE is doing to mitigate the harm, and contact procedures for individuals to ask questions.

iii. **Substitute notice** should be provided as soon as reasonably possible after the Privacy office is aware that it has insufficient or out-of-date contact information for any individual(s). Examples of substitute notice are telephone calls or e-mail notification. If the Privacy Office identifies 10 or more individuals whose information is insufficient or out-of-date (and cannot be updated), a conspicuous posting shall be placed on the home page of the Nebraska Medical Center website for 90 days, or in major print or broadcast media in geographic areas where the individuals affected by the breach are likely to reside. Additionally, a toll-free phone number shall be established, active for 90 days, where an individual can learn whether the individual's unsecured PHI may be included in the breach.

iv. **More than 500 individuals.** If the breach of unsecured PHI involves more than 500 individuals in a single state, the media must be notified (i.e. issue a press release) without unreasonable delay, but within 60 days of discovery of the breach. The media notification must contain the information in 3d(ii) above, and does not substitute for the required individual written notification. Additionally, for breaches of more than 500 individuals, regardless of the number of states in which they reside, the Secretary, U.S. Department of Health and Human Services must be immediately notified.

e. **Breach Notification Log.** The Privacy office shall maintain a breach notification log and submit information required by the Privacy Rule annually to the Secretary of the U.S. Department of Health and Human Services documenting the breaches occurring during the year involved.

4. The Human Resources Department shall maintain a log of all privacy and/or information security-related corrective action taken through its department.

   a. All patient-related incident files shall be maintained for a minimum of six (6) years.

5. When notified of a serious privacy incident with potential liability under HIPAA regulations, the Privacy Officer shall assemble a response team with composition determined by the facts and circumstances of the individual incident. Team members may include (as appropriate):

   a. Administration representative
   b. Representatives from department(s)/division(s) where incident occurred
   c. Human Resources representative if UNMC/UDA workforce breach of confidentiality is suspected/confirmed
   d. Patient Relations representative if patient complaint involved
   e. Public Affairs representative if incident has the potential for public attention and/or if press releases may be required
   f. Risk management representative
   g. Information technology representative
   h. Legal counsel
   i. Campus Security representative
   j. Other representatives as appropriate

6. The response team shall take the following actions:

   a. Create a timeline of events and conduct additional fact finding as necessary.
   b. Determine response(s) to incident and assign responsibilities and timeframe for completion.
   c. Determine if any policies and procedures or processes must be changed to mitigate incident recurrence. Assign responsibility for making changes.

7. The Privacy Officer shall maintain files of privacy incident response team proceedings.

**Definitions**

**Affiliated Covered Entity (ACE)** means legally separate covered entities that designate themselves as a single covered entity for the purpose of HIPAA Compliance. Current Nebraska medical ACE members are: The Nebraska Medical Center, UNMC Physicians, UNMC, University Dental Associates, Bellevue Medical Center, and Nebraska Pediatric.
Practice, Inc. ACE membership may change from time to time. The Notice of Privacy Practices lists current ACE members.

**Breach of unsecured PHI** means the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information. Unsecured PHI is: 1) e-PHI that has not been encrypted; and 2) paper, film or hardcopy PHI that has not been shredded or destroyed, such that it cannot be read or otherwise reconstructed.

**Privacy incident** means an improper use or disclosure of private or confidential information, including proprietary information and protected health information.

**Proprietary information** refers to information regarding business practices, including but not limited to, financial statements, contracts, business plans, research data, employee records and student records.

**Protected Health Information (PHI)** is individually identifiable health information. Health information means any information, whether oral or recorded in any medium, that:
1. is created or received by the Affiliated Covered Entity (ACE); and
2. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Records containing PHI, in any form, are the property of UNMC. The PHI contained in the record is the property of the individual who is the subject of the record.

**Workforce** refers to faculty, staff, volunteers, trainees, students, independent contractors and other persons whose conduct, in the performance of work for the ACE, is under the direct control of the ACE, whether or not they are paid by the ACE.

For more information, see UNMC Policy No. 6045, Privacy, Confidentiality, and Information Security, UNMC Policy No. 6057, Use and Disclosure of Protected Health Information, UNMC Policy No. 6062, Patient/Consumer Complaints, or contact the Privacy Officer.

External Resources for Patients and Consumers / Patient Relations Case Sheet