Live. Learn. Hope.

HIPAA Incidental Uses & Disclosures and Minimum Necessary

NORTHWEST Kidney Centers

www.nwkidney.org

November 2018

Contents

What Does Incidental Use and Disclosure, and Minimum Necessary Mean?

Communications between care providers, and patients and care providers are essential to ensure that patients receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which patient care occurs, the potential exists for an individual's health information to be disclosed incidentally.

An incidental disclosure is a secondary disclosure that:

- Cannot reasonably be prevented;
- Is limited in nature; and
- Occurs because of another use or disclosure that HIPAA does allow.

For example, a hospital visitor may overhear a provider's confidential conversation with another provider or a patient, or one patient may momentarily view another patient's information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices.

HIPAA does not require that all risk of incidental use or disclosure be eliminated. The Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

How the Rule Works

The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure if the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. An incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

Reasonable Safeguards

A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule. It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from all potential risks.

Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. Covered entities should also consider the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing safeguards.

Some examples of reasonable safeguards include:

- Speaking quietly when discussing a patient's condition with family members

in a waiting room or other public area;

- Avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- Isolating or locking file cabinets or records rooms; or
- Providing additional security, such as passwords, on computers.

Minimum Necessary

Covered entities must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. The minimum necessary policy and procedure must reasonably limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business.

For example:

If a hospital employee can have routine, unimpeded access to patients' medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum necessary standard. Therefore, any incidental use or disclosure that results from this practice, such as another worker overhearing the hospital employee's conversation about a patient's condition, would be an unlawful use or disclosure under the Privacy Rule.

The minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes. For example, a physician is not required to apply the minimum necessary standard when discussing a patient's medical chart information with a specialist at another hospital.

Incidental Use and Disclosure

Confidential Conversations That May be Overheard

1. Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

   Answer:

   Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high-quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

   - For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:
   - Health care staff may orally coordinate services at hospital nursing stations.

- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
  - Healthcare professionals may discuss a patient's condition during training rounds in an academic or training institution.
  - A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable.

Phone Messages Left with a Family Member

2. May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?

   Answer:

   Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients at their homes, whether through the mail, by phone or in some other manner. The Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number, and other information necessary to confirm an appointment or ask the individual to call back.

   A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

   In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, a patient request to receive mailings from the covered entity in a closed envelope rather than by postcard to be a reasonable request that should be accommodated.

Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests.

Patient Sign-in Sheets at Physician Offices

3. May physician's offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

   Answer

   Yes. Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called or see other patient names on a sign-in sheet. For example, the sign-in sheet may not display medical information that is not necessary for signing in (e.g., the medical problem for which the patient is seeing the physician).

Medical Charts Outside an Exam Room

4. A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

   Answer:

   Yes, the Privacy Rule permits this practice if the clinic takes reasonable and appropriate measures to protect the patient's privacy. The physician or other healthcare professionals use the patient charts for treatment purposes.

   Incidental disclosures to others that might occur because of the charts being left in the box are permitted if the minimum necessary and reasonable safeguards requirements are met. Since the purpose of leaving the chart in the box is to provide the physician with access to the medical information for the examination, the minimum necessary requirement would be satisfied.

   Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation include:

   - Limiting access to certain areas;
   - Ensuring that the area is supervised;
   - Escorting non-employees in the area; or
   - Placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by.

   Each covered entity must evaluate what measures are reasonable and appropriate in its environment.

Minimum Necessary

Determining Minimum Necessary

1. How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a purpose?

   The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what protected health information is reasonably necessary for a purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard, and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.

   The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards.

   Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.

Exchanges of Patient Information During Treatment

2. Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality healthcare by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

   Answer:

   No. Disclosures for treatment purposes (including requests for disclosures) between healthcare providers are explicitly exempted from the minimum necessary requirements.

   Uses of protected health information for treatment are not exempt from the minimum necessary standard. However, the Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard, and appropriately and reasonably limits access to identifiable health information within the covered entity. The Rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs.

Minimum Necessary Rule & Patient Authorizations

3. Must the HIPAA Privacy Rule's minimum necessary standard to be applied to uses or disclosures that are authorized by an individual?

   Answer:

   No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements. For example, if a covered health care provider receives an individual's authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination.

Uses & Disclosures to Federal or State Agencies

4. Are providers required to make a minimum necessary determination to disclose to Federal or state agencies, such as the Social Security Administration or its affiliated agencies, for individuals' applications for federal or state benefits?

   Answer:

   No. These disclosures must be authorized by an individual and, therefore, are exempt from the HIPAA Privacy Rule's minimum necessary requirements. Use of the provider's own authorization form is not required. Providers can an authorization form if it meets HIPAA requirements.

Using or Disclosing an Entire Medical Record

5. Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time the entire medical record is disclosed?

   Answer:

   No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a covered entity may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

   For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for purposes. The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

   Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who

is the subject of the protected health information.

PHI Created by an Outside Treating Provider

6. A provider might have a patient's medical record that contains older portions of a medical record that were created by another previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

   Answer:

   Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, if the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

Sharing PHI with Another Covered Entity

7. Is a covered entity required to apply the HIPAA Privacy Rule's minimum necessary standard to a disclosure of protected health information it makes to another covered entity?

   Answer:

   Covered entities are required to apply the minimum necessary standard to their own requests for protected health information. One covered entity may reasonably rely on another covered entity’s request as the minimum necessary and then does not need to engage in a separate minimum necessary determination.

   If a covered entity does not agree that the amount of information requested by another covered entity is reasonably necessary for the purpose, it is up to both covered entities to negotiate a resolution of the dispute as to the amount of information needed.

www.nwkidney.org

November 2018