"Addendum B"

HIPAA Guidelines and Information

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
- The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a final Omnibus Rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.

The final Privacy Rule:

- Gives patients more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that healthcare providers and others must achieve to protect the privacy of health information.
- Holds violators accountable, with civil and criminal penalties that can be imposed, if they violate patients' privacy rights.
- Strikes a balance between individual privacy and community responsibility in cases of public health, law enforcement and national security.

The HIPAA Privacy Rule DOES NOT REPLACE any laws that grant individuals even greater privacy protections found in many states. Covered entities are free to retain or adopt more protective policies or practices, as they deem necessary. While most segments of the healthcare industry support the HIPAA objectives of enhanced patient privacy in the healthcare system, they caution that privacy protections must not interfere with a patient's access to or the quality of healthcare delivery.

Incidental Uses and Disclosures
Regarding Incidental Disclosures, the OCR Standards Document answers the following:

"Q. 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. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from

certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of 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.
- Health care 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 situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

"Q. Are physicians and doctor's offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others? "

Answer: No. The HIPAA Privacy Rule does not prohibit covered entity from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual's privacy while engaging in these practices. Covered entities must implement reasonable safeguards to protect an individual's privacy. In addition, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to protected health information. Covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguards to their particular circumstances.

For example, the Privacy Rule does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual's privacy:

- Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., "high fall risk" or "diabetic diet") at patient bedside or at the doors of hospital rooms.

  Possible safeguards may include: reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.

Source: http://www.hhs.gov/hipaa/for-professionals/index.html
Updated by Compliance Department, 1/18/2016

- Announcing patient names and other information over a facility's public announcement system.

  Possible safeguards may include: limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.

- Use of X-ray lightboards or in-patient logs, such as whiteboards, at a nursing station.

  Possible safeguards may include: if the X-ray lightboard is in an area generally not accessible by the public, or if the nursing station whiteboard is not readily visible to the public, or any other safeguard which reasonably limits incidental disclosures to the general public.

The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.

"Q. 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 as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to 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 would be 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. Covered entities may tailor measures to their particular circumstances. See 45 CFR 164.530(c).

"Q. 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. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

Source: http://www.hhs.gov/hipaa/for-professionals/index.html
Updated by Compliance Department, 1/18/2016

"Q. Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?"

Answer: No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

- A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.
- A health plan employee discussing a patient's health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

Minimum Necessity Requirements

Regarding Minimum Necessity Requirements, the OCR Standards Document answers the following:

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

Answer: 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 particular 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.

HIPAA Security Overview

The security regulations jointly developed by HHS Center for Medicare/Medicaid Services (CMS) and the Department of Commerce were released on February 13, 2003 and became effective for most cover entities in April 2005. While the Privacy Rule discussed earlier in this document addressed physical safeguards for protecting patient information in paper documents, the security rule addresses only electronic information. The security rule has been drafted to allow considerable flexibility and discretion in deciding how the security measures will be implemented by a covered

entity. The rule comprehensively covers security regulations for electronic data and distinguishes between "required" and "addressable" measures.

The rule avoids setting specific standards for security. This gives covered entities the opportunity to assess individual risk and determine appropriate implementation specifications best suited to meet the needs of the facility. This lack of specifics also removes the guarantee that a covered entity has achieved total compliance. Much like the Privacy Rule, the Security Rule comes down to commonsense measures to protect patients' medical information, along with comprehensive documentation explaining compliance policies. Organizations that choose to scale down or forgo “addressable” measures are encouraged to take special care to document the bases for their decisions. This documentation is essential since only time will tell what measures the government and the courts will find adequate for compliance with the rule.

Required Measures

This paper does not list all “required” measures of the HIPAA security regulations, focusing primarily on those related to patient charting. Under the new regulations affected, covered entities are required to:

♦ Conduct a thorough risk analysis of their organizations and review electronic information handling procedures, information system activities and policies to develop measures that ensure the integrity of patient health information.

♦ Develop clear policies for detecting and reporting security violations, as well as contingency and disaster recovery plans to guard against patient data loss.

♦ Make business associates and partner companies aware of security policies and procedures, either through written contracts or other less formal means.

While much of the compliance efforts will be the responsibility of the Information Technology (IT) Departments and software vendors (i.e., most physical electronic security measures), a great deal of the responsibility will rest on entity leadership to ensure appropriate policies and procedures are developed and followed. Most healthcare facilities today chart using a combination of electronic and paper methods, giving those caregivers responsibility for approving, granting or obtaining access to electronic patient health information. Use of electronic data will be subject to the new requirements. Specifically, individuals who use electronic patient data will need to understand:

♦ Who has access to electronic protected health information (PHI);

♦ How electronic access to PHI is assigned or changed;

♦ What staff training will be required with regard to electronic security;

♦ Who can change PHI electronic information;

♦ How will electronic records be protected in the event of a disaster;

♦ What steps need to be taken to minimize the chances of electronic record theft;

♦ What proper safeguards and disclaimers need to be in place when PHI needs to be sent electronically (i.e. computer generated or faxed to another party).

Source: http://www.hhs.gov/hipaa/for-professionals/index.html
Updated by Compliance Department, 1/18/2016

Changes in patient charting procedures will depend on existing security and training measures within each entity. How each organization decides to meet the new standards will vary, but what won't vary is the fact that each covered entity is required to review the procedures in place and establish a strategy and action plan to comply. In some institutions, the biggest change will not be in procedures or policy but rather in punishment for breaches in security. Practices, such as granting 'generic logons,' sharing IDs/passwords, or faxing information without first validating destination, although always considered a policy violation in most facilities, will now not only be bad practice, but it may also be considered criminal.

Source: http://www.hhs.gov/hipaa/for-professionals/index.html
Updated by Compliance Department, 1/18/2016