SAFEGUARDS

SAFEGUARDS PRINCIPLE: Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

SAFEGUARDS AND THE HIPAA PRIVACY RULE

The Safeguards Principle in the Privacy and Security Framework emphasizes that trust in electronic health information exchange can only be achieved if reasonable administrative, technical, and physical safeguards are in place. The HIPAA Privacy Rule supports the Safeguards Principle by requiring covered entities to implement appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI). See 45 C.F.R. § 164.530(c). (See also the HIPAA Security Rule at 45 C.F.R. §§ 164.308, 164.310, and 164.312 for specific requirements related to administrative, physical, and technical safeguards for electronic PHI.)

The Privacy Rule's safeguards standard assures the privacy of PHI by requiring covered entities to reasonably safeguard PHI from any intentional or unintentional use or disclosure in violation of the Privacy Rule. The safeguards requirement, as with all other requirements in the Privacy Rule, establishes protections for PHI in all forms: paper, electronic, and oral. Safeguards include such actions and practices as securing locations and equipment; implementing technical solutions to mitigate risks; and workforce training.

The Privacy Rule's safeguards standard is flexible and does not prescribe any specific practices or actions that must be taken by covered entities. This allows entities of different sizes, functions, and needs to adequately protect the privacy of PHI as appropriate to their circumstances. However, since each covered entity chooses the safeguards that best meet its individual needs, the types of protections applied may not be the same across all participants exchanging electronic health information to or through a health information organization (HIO), and some participants may not be covered entities.

When covered entities and others participate in electronic health information exchange with a HIO, the actual exchange of information may be facilitated and even enhanced if all participants adopt and adhere to the same or consistent safeguard policies and procedures. To that end, the flexibility of the Privacy Rule would allow covered entities and the HIO, as their business associate, to agree on appropriate, common safeguards that would apply to their electronic exchange of information. In addition, as a requirement of participation in the electronic health information exchange with the HIO, these commonly agreed to safeguards also could be extended to other participants, even though they are not covered entities. For example, HIO participants may agree to use a common set of procedures and mechanisms to verify the credentials of and to authenticate persons requesting and accessing information through the network or to apply the same standard training for persons who utilize the network.

Common safeguards policies can be formalized through a business associate agreement, data sharing agreement, or any other contract mechanism, and may include enforcement mechanisms and penalties for breaches and violations. A HIO also may establish and centrally control the exchange network, network equipment, and exchange conduits, so that the exchange process itself is protected by a single set of safeguards and security mechanisms.

6627 Valjean Ave.
Van Nuys, CA 91406
Phone: +888-959-0220
Fax: +818-356-7187
Email: info@camhipaasolutions.com
Website: www.camhipaasolutions.com

FREQUENTLY ASKED QUESTIONS

Q1: Does the HIPAA Privacy Rule permit a covered health care provider to email or otherwise electronically exchange protected health information (PHI) with another provider for treatment purposes?

A1: Yes. The Privacy Rule allows covered health care providers to share PHI electronically (or in any other form) for treatment purposes, as long as they apply reasonable safeguards when doing so. Thus, for example, a physician may consult with another physician by e-mail about a patient's condition, or health care providers may electronically exchange PHI to and through a health information organization (HIO) for patient care.

Q2: How may the HIPAA Privacy Rule's requirements for verification of identity and authority be met in an electronic health information exchange environment?

A2: The Privacy Rule requires covered entities to verify the identity and authority of a person requesting protected health information (PHI), if not known to the covered entity. See 45 C.F.R. § 164.514(h). The Privacy Rule allows for verification in most instances in either oral or written form, although verification does require written documentation when such documentation is a condition of the disclosure. The Privacy Rule generally does not include specific or technical verification requirements and thus, can flexibly be applied to an electronic health information exchange environment in a manner that best supports the needs of the exchange participants and the health information organization (HIO). For example, in an electronic health information exchange environment:

- Participants can agree by contract or otherwise to keep current and provide to the HIO a list of authorized persons so the HIO can appropriately authenticate each user of the network.
- For persons claiming to be government officials, proof of government status may be provided by having a legitimate government e-mail extension (e.g., xxx.gov).
- Documentation required for certain uses and disclosures may be provided in electronic form, such as scanned images or pdf files.
- Documentation requiring signatures may be provided as a scanned image of the signed documentation or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law.

Q3: Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

A3: Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In

6627 Valjean Ave.
Van Nuys, CA 91406
Phone: +888-959-0220
Fax: +818-356-7187
Email: info@camhipaasolutions.com
Website: www.camhipaasolutions.com

addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C. Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual's request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated. Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

Q4: Does the HIPAA Privacy Rule allow covered entities participating in electronic health information exchange with a health information organization (HIO) to establish a common set of safeguards?

A4: Yes. The Privacy Rule requires a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), including reasonable safeguards to protect against any intentional or unintentional use or disclosure in violation of the Privacy Rule. See 45 C.F.R. § 164.530(c). Each covered entity can evaluate its own business functions and needs, the types and amounts of PHI it collects, uses, and discloses, size, and business risks to determine adequate safeguards for its particular circumstances. With respect to electronic health information exchange, the Privacy Rule would allow covered entities participating in an exchange with a HIO to agree on a common set of privacy safeguards that are appropriate to the risks associated with exchanging PHI to and through the HIO. In addition, as a requirement of participation in the electronic health information exchange with the HIO, these commonly agreed to safeguards also could be extended to other participants, even if they are not covered entities. A common or consistent set of standards applied to the HIO and its participants may help not only to facilitate the efficient exchange of information, but also to foster trust among both participants and individuals.

Content provided by The Office of Civil Rights