HIPAA Omnibus Rule Is Here: What Do I Do?

Adam Carter Rose, Esq.
Reid and Riege, P.C.
Tel: (860) 240-1065
arose@rrlawpc.com

Overview

What is HITECH?

- The American Recovery and Reinvestment Act of 2009 ("ARRA") was enacted February 17, 2009.
- Title XIII of Division A and Title IV of Division B of the ARRA are known as:
  - The Health Information Technology for Economic and Clinical Health Act ("HITECH")

How Does HITECH Affect HIPAA?

Subpart D of HITECH is entitled "Privacy," and provides for the following:

- Establishes a breach notification requirement.
- Applies HIPAA to business associates directly and expands definition.
- Requires new business associate obligations to be incorporated into business associate agreements.

How Does HITECH Affect HIPAA? (cont.)

- Creates government obligations to provide education on HIPAA.
- Amends Privacy Rule in certain respects:
  - Patients can restrict disclosure to health plans under certain circumstances.
  - New “minimum necessary” standard.
  - Electronic health record accounting of disclosures must include disclosures for treatment, payment, and health care operations for the 3 years prior to the request.

How Does HITECH Affect HIPAA? (cont.)

- Amends Privacy Rule in certain respects (cont.):
  - Patients must be granted access in an electronic format to electronic health record (limits charge to labor costs).
  - Prohibits sale of protected health information except in very limited circumstances.
  - Refines “health care operations” as related to marketing.
  - Requires patient to be provided opportunity to opt out of fundraising.

How Does HITECH Affect HIPAA? (cont.)

- Establishes separate breach notification requirements for personal health record vendors.
- Enhances enforcement.
  - Applies criminal penalties to individuals and employees.
  - Grants states' Attorney Generals enforcement authority.
  - Requires investigation of certain complaints.
  - Significantly increases civil monetary penalties.
  - Requires periodic government audits.
  - Provides for individuals to receive portion of civil monetary penalties.

So what do I do?

Action Steps

- ❑ Amend HIPAA policies and procedures.
- ❑ Amend HIPAA privacy notice.
- ❑ Amend all business associates agreements.
- ❑ Provide additional employee training as necessary and appropriate.
- ❑ Document all of the foregoing in preparation for an audit or to respond in the event of an investigation.

Privacy Policies and Procedures

"A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law." 45 C.F.R. § 164.530(i)(2).

Privacy Policies and Procedures
Breach Notification – HITECH § 13402

STEP 1: Add a breach notification policy and procedure.

Prior Law: No prior HIPAA regulation. Connecticut law contains an electronic breach law. Conn. Gen. Stat. § 36a-701b.

Compliance Date: September 23, 2009, enforcement postponed to February 22, 2010.

Privacy Policies and Procedures
Breach Notification – HITECH § 13402

Covered entities and business associates now have certain notification obligations when there is a "discovery" of a "**breach**" of "**unsecured protected health information**."

Personal health record vendors have separate reporting obligations.

Privacy Policies and Procedures
Breach Notification – 45 C.F.R. § 164.402

"Unsecured" means the PHI is not "rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology as specified by the government.

- ❑ The standard is generally that PHI must be encrypted or destroyed in order to be considered secure.
- ❑ See, 74 Federal Register 42741-43 (August 24, 2009) for a more detailed description of the standards.

Privacy Policies and Procedures
UPDATE – Breach Notification – 45 C.F.R. § 164.402(1)

- As of September 23, 2013, a "breach" is any unintentional acquisition, access, use, or disclosure of PHI not permitted by the HIPAA Privacy Rule.
- Any such acquisition, access, use, or disclosure is presumed to be a breach unless the covered entity or business associate demonstrates a low probability that PHI has been compromised.
  - No longer limited to situations where breach poses a significant risk of financial, reputational, or other harm to the individual

Privacy Policies and Procedures
UPDATE – Breach Notification – 45 C.F.R. § 164.402(2)

- To demonstrate a low probability that PHI has been compromised, a risk assessment must be performed based on at least these factors:
  - Nature and extent of PHI involved and the types of identifiers and 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
  - Extent to which risk to PHI has been mitigated

Privacy Policies and Procedures
Breach Notification – 45 C.F.R. §§ 164.404-410

- Business associate notifies covered entity.
- Covered entity notifies:
  - Affected Individuals
    - In writing or by other means if necessary.
  - U.S. Department of Health and Human Services
    - Either annually or immediately if breach involves more the 500 individuals.
  - The Media, if more than 500 residents in a state are affected.

Privacy Policies and Procedures
Breach Notification – 45 C.F.R. § 164.404(c)

The notice to individuals must include, to the extent possible, a description of:

- What happened, including the date of the breach;
- The unsecured PHI subject to the breach;
- Recommended steps for individuals to take to mitigate potential harm;
- What the covered entity is doing in response; and
- Contact procedures, which shall include a toll-free telephone number, an email address, website, or postal address.

Privacy Policies and Procedures
Breach Notification – 45 C.F.R. §§ 164.410-412

Timing of Notification is without unreasonable delay but not later than 60 days after "discovery."

- Discovery is the first day it is known or would have been known if covered entity/business associate used reasonable diligence.
  - Applies to any workforce member or agent (per federal common law of agency) (other than person committing the breach)
- Immediate notice to HHS if breach involves more than 500 people. Otherwise, annual log will suffice.
- Subject to law enforcement delay.
- Burden on organization to prove timeliness.

Privacy Policies and Procedures
UPDATE – Breach Notification – 45 C.F.R. § 164.402

Summary of Step 1: Update your breach notification policy and procedure to remove the element of significant harm and replace with the process of performing a risk assessment for the purpose of determining whether there is a "low probability that the protected health information has been compromised."

Privacy Policies and Procedures
UPDATE – Restrictions – 45 C.F.R. § 164.522(a)(1)(vi)

STEP 2: Amend disclosure restriction policies and procedures to provide that patients can restrict disclosures to health plans for payment and health care operations when the patient had paid for the item or service subject to the restriction out of his or her own pocket.

Prior Law: Covered entities are not required to honor patient requested restrictions. 45 C.F.R. § 164.522(a)(1)(i-ii).

Compliance Date: February 17, 2010.

Privacy Policies and Procedures
Minimum Necessary – HITECH § 13405(b)

STEP 3: Amend minimum necessary standard to require that, to the extent practicable, any use, disclosure, or request for PHI is limited to PHI in a "limited data set," until the government issues superseding guidance. The covered entity must decide the minimum necessary.

Prior Law: Minimum necessary to be determined by covered entity, except it may reasonably rely on requests for disclosures under certain circumstances. 45 C.F.R. § 164.514(d).

Compliance Date: February 17, 2010.

Privacy Policies and Procedures
UPDATE – Minimum Necessary – 45 C.F.R § 164.502(b)(1)

- Minimum necessary standard is now also applicable to disclosures with and between business associates

Privacy Policies and Procedures
EHR Accounting – HITECH § 13405(c)

STEP 4: Amend accounting of disclosure policy to provide that requests for an electronic health record accounting of disclosures must include disclosures for treatment, payment, and health care operations for the 3 years prior to the request.

Only applies if the covered entity maintains an electronic health record.

Covered entity may decide to account for business associate or give patient business associate's contact information.

Prior Law: No accounting requirement for treatment, payment, and healthcare operations. 45 C.F.R. § 164.528(a)(1)(i).

Compliance Date: If EHR acquired prior to January 1, 2009, then January 1, 2014. For subsequent acquisitions of EHR, the earlier of the point of acquisition or January 1, 2011.

Privacy Policies and Procedures
UPDATE – EHR Accounting

- Guidelines on EHR accounting will be provided in a later rule
  - 78 Fed. Reg. 5568 (January 25, 2013).

Privacy Policies and Procedures
UPDATE – Sale of PHI – 45 C.F.R. § 164.502(a)(5)(ii)

STEP 5: Add a policy that prohibits receipt of any remuneration, either directly or indirectly, in exchange for PHI or electronic health records unless the patient signs a written "authorization" that also indicates whether the PHI can be further exchanged for remuneration by the entity or person to whom the PHI is originally sold.

Does not apply to treatment of the individual, health care operations of the covered entity, payment to business associates to carry out actions on behalf of covered entity, and providing a copy to the individual.

There are a number of other exceptions that provide for the sale of PHI, but these need to be carefully reviewed and incorporated into a policy only if relevant (i.e. sale of PHI for research purposes).

Privacy Policies and Procedures
UPDATE – Sale of PHI – 45 C.F.R. § 164.502(a)(5)(ii)

STEP 5 (cont.): Prohibit sale of PHI...

Prior Law: Not addressed.

Compliance Date: September 23, 2013

Privacy Policies and Procedures
UPDATE – Electronic Access – 45 C.F.R. § 164.524(c)(2)

STEP 6: Amend patient access policy and procedure to provide that patients must be granted access to their electronic health records in an electronic format.

Request may direct that the information be sent to an entity or person, provided the request is clear, conspicuous, and specific.

Only applies if covered entity maintains an electronic health record.

Limits charges for access to labor costs.

Prior Law: Patient access provision does not address electronic health record access. 45 C.F.R. § 164.524.

Compliance Date: February 17, 2010.

Privacy Policies and Procedures
UPDATE – Marketing – 45 C.F.R. § 164.508(a)(3)(ii)

STEP 7: Amend any policy, or add a policy, stating that covered entity shall not accept payment directly or indirectly for sending a marketing communication.

If the covered entity intends upon receiving a payment for sending a marketing communication, it should then review the statutory exceptions that outline the strict circumstances under which such communications are permitted.

Prior Law: Use of PHI for marketing purposes requires a patient "authorization," except for face-to-face communications, or promotional gifts of nominal value. If remuneration to the covered entity is involved, this must be disclosed to the patient. 45 C.F.R. § 164.508(a)(3).

Compliance Date: February 17, 2010.

Privacy Policies and Procedures
UPDATE – "Marketing" Definition – 45 C.F.R. § 164.501

- Treatment and health care communications are now included in the definition of marketing where the covered entity receives financial remuneration.

Privacy Policies and Procedures
UPDATE – Fundraising Opt Out – 45 C.F.R. § 164.514(f)(2)

STEP 8: If the policy does not already so provide, amend to ensure that each fundraising communication provides a clear and conspicuous opportunity for patients to elect not to receive any further fundraising communications.

It will be a violation to send a fundraising communication to an individual who has opted out. You may provided a procedure to opt back in.

Prior Law: Same opt out requirement, but covered entities only had to make "reasonable efforts" to honor the opt out election. 45 C.F.R. § 164.514(f)(2).

Compliance Date: February 17, 2010.

Privacy Policies and Procedures UPDATE – Business Associates – 45 C.F.R. §§ 164.314(a)(2)(i) and 164.504(e)(2)

STEP 9: Amend any existing policy or procedure relating to business associates to ensure that there is a written Omnibus Rule compliant business associate agreement delineating the respective rights and obligations (as discussed later in this presentation).

Prior Law: The required terms of a business associate agreement are set forth in 45 C.F.R. §§ 164.314(a)(2)(i) and 164.504(e)(2).

Compliance Date: Either September 23, 2013 or September 22, 2014 (to be discussed).

Privacy Notice

"The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses and disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice." 45 C.F.R. § 164.520(b)(3).

UPDATE – Privacy Notice

Use and implement the "model" notice by September 23, 2013

UPDATE – Privacy Notices

Notice revisions for September 23, 2013

- Add right to restrict disclosures to health plans
- Add right to be notified of breaches of unsecured PHI (if not already)
- Include statement that authorization is required for:
  - Marketing involving payments to covered entity
  - Disclosures that constitute a sale of PHI
  - Uses and disclosures of psychotherapy notes
    - With certain limited exceptions
  - Any other uses or disclosures not described in the notice
- Add right to opt out of fundraising communications

Business Associate Agreement Omnibus Rule Compliance

Business Associate Agreement UPDATE – 45 C.F.R. § 164.532

Compliance Deadlines

- If a business associate agreement was entered, modified, or renewed on or after January 25, 2013, the business associate agreement must also comply with the new requirements by September 23, 2013.
- An agreement entered into prior to January 25, 2013 and not renewed or modified between March 26, 2013 and September 23, 2013, may be grandfathered if it complied with the regulations effective on the date it was entered.
  - Will be valid until the contract is modified or renewed after September 23, 2013 or until September 22, 2014, whichever occurs earlier.

Business Associate Agreement UPDATE – 45 C.F.R. §§ 164.314(a)(2)(i) and 164.504(e)

Revisions for September 23, 2013 or September 22, 2014

- Specify that business associate agrees to comply with administrative, physical, and technical safeguards, and policies and documentation requirements of the Security Rule.
- Add a provision that specifies that if a covered entity delegates an obligation to the business associate under the Privacy Rule the business associate must comply with the Privacy Rule in carrying out that obligation.
- Specify the need for business associate agreements between business associates and subcontractors.
- Address breach notification (although already required).

Questions and Comments

Disclaimer

This presentation is being offered for educational purposes only. While it provides information on recent developments, you are urged not to take action based solely on its contents.

Thank You

Adam Carter Rose
Reid and Riege, P.C.
Tel: (860) 240-1065
arose@rrlawpc.com