

Privacy Changes in the HITECH Act


Mary Thomason, RHIA, CHPS, CISSP



Disclaimer

- ▶ This is not legal advice. Always consult your own legal counsel!


Impact of the HITECH act on privacy compliance

- ▶ Health Information Technology for Economic and Clinical Health (HITECH) Act is part of the American Recovery and Reinvestment Act of 2009, signed in February
 - ▶ Included privacy provisions will have significant impacts on privacy and security compliance now and in the coming years
 - ▶ First major changes to HIPAA Privacy rule
- 

Major immediate impacts

- ▶ OLD HIPAA: Fines for privacy and security violations of HIPAA had a cap of \$100/ violation, maximum of \$25,000 per violation type.
- ▶ OLD HIPAA: Had limitations that the Secretary of HHS could not apply penalties– if the covered entity did not know, and could not reasonably have known they were in violation, if the failure was due to a reasonable cause, and it was corrected in 30 days.

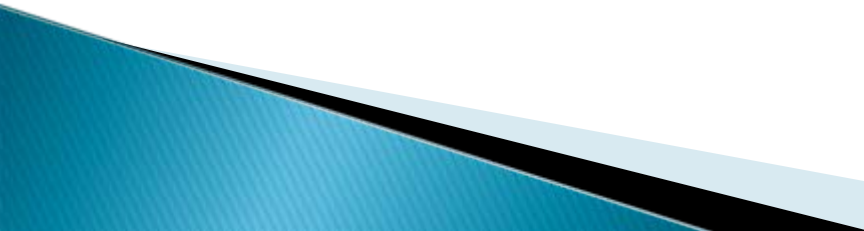
Penalty impacts

- ▶ Fines can be applied for any violations on or after February 18, 2009.
 - ▶ Now fines are a minimum of \$100, and depend on “level of culpability”
 - ▶ Maximum fines per violation of identical provisions per calendar year is \$1.5 million
- 

Categories of Violations

Violation Category	Each Violation	Maximum for all violations of identical provisions per year
Did not know	\$100–\$50,000	\$1,500,000
Reasonable Cause	\$1,000–\$50,000	\$1,500,000
Willful Neglect–Corrected	\$10,000–\$50,000	\$1,500,000
Willful Neglect–Not Corrected	\$50,000	\$1,500,000

In place NOW

- ▶ Patients must be informed in writing by covered entities of breaches of their protected health information as soon as possible, but at least in 60 days of the date of discovery of the breach
 - ▶ Business associates must inform covered entities of breaches
 - ▶ Covered entities must also inform the Secretary of Health and Human Services and the local news media at the same time when there are 500 or more individuals involved in the breach
- 

What is a “breach”?

- ▶ The acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the Privacy rule which *compromises the security or privacy of the protected health information.*
- ▶ Compromises the security or privacy of the protected health information means *poses a significant risk of financial, reputational or other harm to the individual.*


Not considered breaches

- ▶ Unintentional use of PHI by workforce or a business associate done in good faith, within the scope of the person's job, and does not result in further impermissible use or disclosure (e.g. employee sends email with PHI to wrong employee)
- ▶ Inadvertent disclosure of PHI from one person to another where both may access PHI, and is part of the same covered entity, business associate or organized health care arrangement (e.g. HIM person faxes H&P to wrong affiliated clinic)

Not considered breaches

- ▶ Unauthorized disclosure in which the recipient would not reasonably have been able to retain the information (e.g. EOB mailed to wrong address, returned unopened)


Breach notification

- ▶ Breach notification must be made starting with any breaches identified on or after September 23, 2009
 - ▶ The clock starts ticking for the report as soon as any employee of the covered entity knows about the breach
 - ▶ Breaches can be of protected health information in any media– e.g. verbal, electronic, or on paper
 - ▶ Documentation very important– what was reported, when, how incident was assessed, when notification was sent or why it was not sent
- 


Starting in February– still pending regulations

- ▶ If patients request it, covered entities cannot send information about a health care related service or item to their health plan, if they pay for the service out of pocket.
- ▶ Disclosures of PHI should be limited to a “limited data set” when practical. If not, the covered entity must determine what is the minimum necessary and only disclose that–cannot depend on the requestor to make that determination as in the past. The Secretary may provide guidance on what is the minimum necessary for various purposes.

Starting in February–still pending regulations

- ▶ Patients must be able to obtain copies of their electronic records in electronic format if they ask for it, or have the information forwarded in electronic format to a third party.
 - ▶ Certain communications that may have been considered health care operations before by a covered entity will have to be considered marketing (will need authorizations)
 - ▶ New restrictions on “sale of protected health information”
- 

Starting in February– still pending regulations

- ▶ If a patient opts out of contacts for fundraising, it must be treated as a revocation of authorization– not just “try your best” not to contact the patient again
 - ▶ Business associates will be under the Privacy Rule in their use of PHI; and must meet the Security Rule standards to protect e-PHI. They also are under the penalty structure as covered entities.
- 

Starting in February

- ▶ Health Information Exchanges, Regional Health Information Organizations, e-Prescribing Gateways, or personal health record vendors who provide a personal health record for covered entities are now to be considered business associates.

Coming attractions

- ▶ Accounting of disclosures requirements will need to include disclosures from electronic health records for treatment, payment or health care operations for three years. Compliance dates may be dependent on when the covered entity acquires their EHR.
- ▶ (This is in addition to the existing accounting of disclosure requirements for any disclosures outside of treatment payment, healthcare operations, to the patient, or by authorization that must be kept for six years).

Questions?

