THINGS TO UPDATE – final rule available at <https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-290>

**When must a provider abide by a patient’s request to not disclose health information?**

Requires a covered entity to agree to a request to restrict disclosure of protected health information to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full. This is an exception to the general rule that a covered entity is not required to agree to a request for restrictions on the use or disclosure of protected health information allowed under the Privacy Rule. (HIPAA Privacy Rule § 164.522(a)(1)(vi)(B)).

**When may a provider accept money for health information?**

The HITECH Act explicitly prohibits the sale of PHI,[[1]](#footnote-1) and specificly states that this prohibition extends to electronically stored health information[[2]](#footnote-2) (Electronic Health Records, or “HER”).

There are, however, several exceptions to this prohibition. Thus, a covered entity may, without an authorization, receive remuneration in exchange for protected health information for:

• Public health activities;

• Research, provided that the amount of remuneration reflects the costs

of preparation and transmittal of the protected health information;

• Treatment;

• “[S]ale, transfer, merger, or consolidation of all or part of the covered

entity with another covered entity . . . and due diligence related to such

activity,” *see* 45 C.F.R. § 164.501 (“health care operations” ¶ (6)(iv));

• Remuneration paid to a business associate for conducting activities “at

the specific request of the covered entity [and] pursuant to a business

associate agreement”;

• An individual’s copy of his/her own protected health information in a

designated record set, pursuant to 45 C.F.R. § 164.524; and

• Other purposes permitted by HHS regulation.

A covered entity may sell protected health information pursuant to an authorization that

acknowledges receipt of remuneration. 45 C.F.R. § 164.508(a)(3)(ii). A covered entity may also

include protected health information in the “sale, transfer, merger, or consolidation of all or part of

the covered entity with another covered entity . . . and [may use and disclose protected health

information for] due diligence related to such activity.” 45 C.F.R. §§ 164.501 (“health care

operations” ¶ (6)(iv)), 164.502(a)(1)(ii).

Earlier this year, the Department of Health and Human Services (HHS) published a final rule, changing parts of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. Some of these are changes required by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act or by the Genetic Information Nondiscrimination Act (“GINA”). These two laws, and the changes adopted by the final rule, reflect the health industry’s growing reliance on electronically stored information, as well as Congress’s concern for patient information to be kept safe.

Notably, HITECH changes HIPAA’s data breach notification requirements, requirements for business associates, restrictions on marketing, revision of the minimum necessary standard, restrictions on the sale of protected health information and Electronic Health Records, requirements for certain requests to restrict use or disclosure of protected health information, provisoin related to Electronic Health Records, and enhanced enforcement of HIPAA Privacy and Security provisions.

Penalties:

Civil/monetary penalties imposed for violating HIPAA rules comes from HIPAA Enforcement Rule. Now there is an increased and a four-level tiered civil money penalty structure provided by the HITECH Act (78 FR 5567 (Jan. 25, 2013)). Penalties are now assessed depending on the covered entity’s culpability; the minimum penalty amount for each violation has been increased to $100 for each HIPAA violation, and the maximum penalty has been set at 1.5 million dollars annually. (HITECH Act §§ 13410(d)(1)(C)(ii); (d)(3)(D) (42 U.S.C. §§ 17939(d)(1)(C)(ii); (d)(3)(D))) 78 FR 5577 (Jan. 25, 2013). Additionally, covered entities may no longer avoid monetary penalties by using the affirmative defense that they did not know (and would not have known if they had been reasonably diligent) of the violation. (HITECH Act § 13410(d)(4)). Previously, the Secretary could not impose a monetary penalty if the covered entity could demonstrate that it did not know and could not have known of the violation. 45 C.F.R. § 160.410(b)(2).

State Attorney Generals may now bring civil actions on behalf of the residents of the state, if it can be shown that the residents were harmed by a covered entity’s non-compliance. (HITECH Act § 13410(e) (42 U.S.C. § 17939(e))).

Civil and Criminal enforcement of HIPAA rules – Health Information Technology for Economic and Clinical Health (HITECH act)

Breach notification from HITECH -> Breach Notification Rule, implemented through interim final regulations that were effective on Sept 23, 2013. Establishes standards for providing notification of breaches of unsecured PHI.

Covered Entities must now change their policies and procedures to reflect the definition of breach and explaining when patients will be notified of a breach.

What a breach is 🡪 A breach can refer to any acquisition, access, use, or disclosure of patient information (be it the patient’s name, address, SSN, or other identifying information (45 C.F.R § 164.514(b)(2)) or health information (45 C.F.R § 160.103)) in a manner not permitted under the Privacy Rule. There is a presumption that any impermissible use or disclosure of such information constitutes a breach which requires the covered entity to notify the proper parties. (45 C.F.R. 164.402(1)).

The covered entity may overcome this presumption by demonstrating that there is “a low probability” of risk that the information has been compromised. Patients must be notified of a breach, therefore, in every situation when PHI is acquired, accessed, used, or disclosed in a manner not permitted under the Privacy Rule, *except* when a covered entity (or Business Associate, when applicable) demonstrates that there is a low probability that the PHI has been compromised, using an objective risk assessment, based upon at least the following four factors, unless regulatory exclusions apply (see exclusions discussed in the next paragraph): (

(*See* definition of breach at 45 C.F.R. §§ 164.402(2)(i)-(iv)). )

1. “the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification,
2. The unauthorized person who used the PHI or to whom the disclosure was made,
3. Whether the PHI was actually acquired or viewed, and
4. The extent to which the risk to the PHI has been mitigated.

The covered entity should document and retain the risk assessment in which they engage, and should note additional factors they considered when assessing the risk.

Exclusions; what *isn’t* considered a breach: There are three exceptions to the general rule:

1. The unintentional use of the information by member of the covered entity’s workforce (*See* definition of breach at 45 C.F.R. 164.402(1)(i)).
2. Inadvertent disclosure by the covered entity to authorized person (*See* definition of breach at 45 C.F.R. 164.402(1)(ii)).
3. When the recipient does not retain the protected health information (*See* definition of breach at 45 C.F.R. 164.402(1)(iii)).

It should be noted that the final rule has removed a prior exception that existed for the disclosure of data, so long as the disclosed information did not include any dates of birth or zip codes. Now, a covered entity should always perform a risk assessment after any improper use or disclosure of information to determine whether a breach notification should be given.

Notification: When a covered entity discovers a breach, it is required to notify the affected individuals, HHS, and – if appropriate – the media. A covered entity needs to keep a record of discovered breaches affecting less than 500 patients, which is submitted each year to HHS. It should be noted that this is a change from what the law required before – prior to the Final Rule, the log was submitted within 60 days after the end of the calendar year for breaches that occurred during the immediately preceding calendar year, but now the log is submitted within 60 days after the end of the calendar year for breaches that were discovered during the immediately preceding calendar year.

The covered entity is ultimately responsible for notifications, regardless of any business associate involvement or fault. Business associates are responsible only for informing the covered entity of any discovered breach. Media outlets are not required to print or broadcast these notifications, and covered entities are not required to pay for notifications to be printed or broadcasted. Covered Entities are, however, required to deliver notice, such as a press release, directly to the prominent media outlets being notified. It will not fulfill the notice requirements to simply post a press release to the covered entity’s website. Finally, in the event that a notice to a patient is returned to the covered entity as undeliverable, either direct written notice using updated contact information or substitute notice (consistent with regulatory guidelines) must be given within the original 60-day deadline. §

BUSINESS ASSOCIATES

What is a business associate? The new changes have expanded the kinds of entities that are considered business associates, and makes business associates directly liable for certain HIPAA violations. Any person or entity (other than a member of the covered entity’s workforce) who creates, receives, maintains, or transmits PHI on behalf of the CE is considered a business associate. The new changes have added the word “maintains” to the definition, so that entities that never or infrequently view the PHI they maintain are still responsible for its security. This will include subcontractors. Covered entities are not required to enter into Business Associate Agreements with subcontractors, but the business associate *is* required to do so.

Genetic Information Nondiscrimination Act of 2008 (GINA) – People have until sept 23rd, 2013 to comply. Strengthens HIPAA privacy protections for genetic information.

1. HITECH Act § 13405(d) (42 U.S.C. § 17935(d)). [↑](#footnote-ref-1)
2. HITECH Act § 13405(d) (42 U.S.C. § 17935(d)). [↑](#footnote-ref-2)