



MetLife

© UFS

Jurisdiction	Effective Date	Author	Release Date	File No.
Federal	3/26/13	Michael F. Tietz Louis Enahoro	2/12/13	LI-457
Topic	HIPAA, Privacy, Privacy Notification			
Citation:	45 CFR Parts 160 and 164			
Reference:	Supplements LI-187, LI-202, LI-221, LI-233, LI-308, LI-355, LI-374, LI-386, LI-388			

HHS ISSUES NEW HIPAA PRIVACY AND SECURITY OMNIBUS RULE

Executive Summary

The U.S. Department of Health and Human Services (HHS) has issued its long-awaited omnibus final rule covering HIPAA privacy and security enforcement, security breaches and genetic information (“Omnibus Rule” or “Final Rule”).

Among other things, the Omnibus Rule makes significant changes in the following areas:

- Makes business associates directly liable for compliance with HIPAA privacy and security requirements and reconfirms the requirement to enter into a business associate agreement;
- Imposes new requirements on the use and disclosure of protected health information for marketing and fundraising purposes;
- Prohibits the sale of protected health information without individual authorization;
- Gives individuals the right to receive electronic copies of their protected health information from health plans and designate its transmission to third parties;
- Gives individuals the right to restrict disclosure of protected health information to health plans for services paid out-of-pocket in full;
- Requires covered entities to modify and redistribute their HIPAA privacy notices;
- Changes the HIPAA security breach rules to require a formal risk assessment;
- Confirms the new four tier penalty structure and other enforcement provisions set out in the Health Information Technology for Economic and Clinical Health Act (HITECH); and
- Prohibits health plans, except Long Term Care (LTC) plans, from using or disclosing genetic information for underwriting purposes.

In general, all covered entities must be in compliance with the rule's new requirements by September 23, 2013. The Final Rule also extends the compliance date for modifying certain business associate agreements and distributing privacy notices.

Background

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996.¹ HIPAA's "administrative simplification" provisions are intended to improve the efficiency and effectiveness of the health care system by requiring health care providers, health plans and health care clearinghouses to use uniform standards when processing health care transactions electronically, while at the same time safeguarding the health information contained in these transactions.

HIPAA requires HHS to issue regulations adopting uniform standards for electronic health care transactions, privacy, security and unique identifiers. Prior Legislative & Regulatory Information releases have described and analyzed regulations issued by HHS relating to HIPAA. See Releases LI-179R (electronic transactions); LI-187 (privacy); LI-202 (HHS privacy guidance); LI-207 (ASCA EDI delay law); LI-217 (standard employer identifier); LI-221 (modifications to privacy rule); LI-233 (security); LI-236 (EDI modifications); LI-243 (HHS EDI guidance); LI-261 (national provider identifier); LI-308 (final enforcement rule); LI-326 (contingency plans for national provider identifier); LI-374 (federal stimulus law); LI-376 (electronic transaction standards modifications); LI-377 (ICD-10); LI-386 (PHI technical safeguards); LI-388 (security breach guidelines); and LI-449 (HPID, delay of ICD-10 compliance date & national provider identifier changes).

Congress passed the Genetic Information Nondiscrimination Act (GINA)² in 2008 to prevent health plans from using genetic information in underwriting or to discriminate against employees. GINA also required HHS to revise the HIPAA privacy rule to treat genetic information confidentially.

In 2009 Congress passed the HITECH Act, which contains new HIPAA privacy and security requirements.³ HITECH also required HHS to issue implementing regulations.

HHS issued the Omnibus Rule on January 25, 2013, which implements the requirements of HITECH and GINA.⁴

Significant Terms

Business Associate (BA): A person or company (including a vendor, TPA or other entity) which provides services for or on behalf of covered entities relating to protected health information.

Examples of business associates include companies that engage in claims processing or administration, billing, data analysis, or that provide legal, actuarial, accounting, data aggregation, management, administrative, accreditation or financial services to covered entities. Under the

¹ P.L. 104-191.

² P.L. 110-233; 42 U.S.C. §§ 2000ff-2000ff-11.

³ P.L. 111-5; 42 U.S.C. §§ 1320d-1320d-9.

⁴ See 45 C.F.R. Parts 160 and 164; 78 F.R. 5565-5702.

Omnibus Rule, BAs also include health information organizations, personal health record vendors and data transmission vendors.

Genetic Information: Any information about a genetic test (such as DNA or RNA analysis) of an individual or an individual's family members, as well as the existence of a family member's genetic disease or disorder. Genetic information applies to the fetus or embryo of a pregnant woman. The following are not considered to be genetic information: the disease, age or gender of an individual.

HIPAA Covered Entity (CE): A health plan, health care clearinghouse or health care provider which transmits any health information in an electronic form to perform a transaction covered by the HIPAA privacy rule.

Protected Health Information (PHI): Individually identifiable health information that is maintained or transmitted in any form or medium (whether electronic, written or oral) by CEs and BAs, with a few specified exceptions.

Security breach: The acquisition, access, use, or disclosure of PHI which compromises the security or privacy of PHI, unless it meets specified narrow exceptions, or unless a risk assessment determines a "low probability" that PHI has been compromised.⁵

Subcontractor: A person or company to whom a BA delegates a function, activity, or service involving PHI. A Subcontractor does not include a BA's employee.

Unsecured PHI: PHI that is not secured through the use of a technology or methodology specified by HHS that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals.

Analysis

What the Omnibus Rule Does: The Omnibus Rule changes existing rules related to HIPAA privacy and security, breach notification, HIPAA enforcement, and use and disclosure of genetic information. Highlights of some of the more significant provisions are addressed below.

Privacy & Security Requirements

Business Associates: The Omnibus Rule expands the current definition of BAs to add Subcontractors, health information organizations, personal health record vendors, electronic prescribing gateways and other entities that offer data transmission services on a routine basis.⁶

The Final Rule imposes new obligations on BAs:

- BAs will now need to comply with the HIPAA Security rule. This will require BAs, among other things, to implement administrative, technical and physical safeguards to protect PHI, perform a risk analysis, appoint a security official, comply with security breach notification provisions, and create appropriate policies and procedures.⁷

⁵ See Legislative & Release Information release 388 for more information on the three exceptions.

⁶ See 78 F.R. 5570-5571 for a discussion by HHS of data transmission vendors and services.

⁷ Where a BA causes a security breach, a CE may also be liable for the breach if the BA is acting as an "agent" of the CE.

- BAs will be directly subject to most of the provisions of the HIPAA Privacy rule.⁸
- BAs will be subject to investigations by HHS of HIPAA complaints and violations, and to imposition of HIPAA civil monetary penalties.
- BAs will need to enter into business associate agreements with their Subcontractors by the compliance date (September 23, 2013).

Of note, the Final Rule clarifies that the definition of “workforce” now covers a BA’s workforce, including employees, trainees, and temporary personnel. The HHS commentary indicates that, among other things, BAs will need to train their workforce members as necessary to comply with HIPAA requirements.⁹

Covered Entities will need to review their existing BA agreements to make sure they comply with these new requirements. For BA agreements in existence prior to January 25, 2013, CEs and BAs will have until September 22, 2014 to revise their existing agreements. Until that time, CEs and BAs can continue to operate under their existing BA agreements.

For new BA arrangements arising after January 25, 2013, CEs and BAs will have until September 23, 2013 to finalize BA agreements that comply with the Final Rule.

Marketing: The Omnibus Rule tightens HIPAA’s marketing requirements where a CE or BA receives “financial remuneration”¹⁰ from a third party in exchange for making a marketing communication to a HIPAA-covered individual. In such cases, the CE or BA will need to have a signed authorization from the individual before sending the communication.

However, no authorization will be needed for the following communications, even when the CE or BA may receive financial remuneration:

- Face-to-face communications related to treatment or health care operations, even if financial remuneration is received from a third party;
- Promotional gifts of a nominal value;
- Refill reminders;
- Communications relating to government and government-sponsored programs; and
- General health communications that do not promote a product or a service from a particular provider.¹¹

Sale of PHI: HITECH prohibits a CE or BA from receiving payment in exchange for the disclosure of PHI without a valid authorization.¹² The Final Rule clarifies that a “sale of PHI” is the disclosure

⁸ Other than the privacy and security obligations specified in the Omnibus Rule, BAs will only be responsible for those obligations contained in the BA agreement. For example, BAs are not required to send out HIPAA privacy notices or designate a HIPAA privacy officer.

⁹ See 78 F.R. 5630.

¹⁰ 45 C.F.R. §§ 164.501 and 164.508(a)(3)(ii). The HHS commentary explains that financial remuneration includes only payments made in exchange for making such communications. It does not include non-financial benefits (e.g., in-kind benefits) provided to a CE in exchange for making a communication about a product or service. See 78 F.R. 5596.

¹¹ 45 C.F.R. § 164.508(a)(3)(i)(A) and (B); Section 13406 of the HITECH Act and 78 F.R. 5597.

¹² Section 13405(d) of the HITECH Act; 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(1) and 164.508(a)(4)(i).

of PHI made in exchange for either financial or nonfinancial benefits.¹³ However, the following activities are not considered to be a “sale”:

- disclosures for public health purposes;
- disclosures for research purposes;
- disclosures for treatment and payment purposes;
- sale, transfer or merger activity;
- activities performed by a BA on behalf of a CE;
- responding to an individual’s request; and
- disclosures required by law.¹⁴

Disclosure of Decedent Records: Individually identifiable information of a person who has been deceased for more than fifty years is no longer considered PHI under the Final Rule. Decedent PHI may be disclosed by a CE to family members involved in the care or payment for care of the decedent prior to his/her death, unless it is known to the CE that the decedent would have objected to the disclosure.¹⁵

Right to Request Restrictions: Under the Omnibus Rule, individuals may restrict the disclosure of PHI to a health plan where the individual has paid a provider out-of-pocket and in full for treatment received.¹⁶

Access Rights to PHI in Electronic Format, and designation to Transmit to Third Parties: The Omnibus Rule gives individuals the right to receive a copy of their PHI from CEs in electronic format upon request.¹⁷ An individual can also direct a CE to send an electronic copy of his or her PHI directly to a third party.¹⁸ CEs must implement reasonable safeguards to protect electronic information, and may charge reasonable fees which cover the costs of providing electronic records.

HIPAA Privacy Notices: Covered Entities will need to modify and update their HIPAA privacy notices to include a number of additional provisions, where applicable:

- A description of the types of uses and disclosures that require an authorization, that other uses and disclosures not described in the notice will only be made with an individual’s authorization, and that authorizations may be revoked.¹⁹
- If a CE engages in fundraising, an explanation of fundraising communications and the individual’s right to opt-out of receiving such communications.

¹³ 45 C.F.R. § 164.502(a)(5)(ii)(B)(1).

¹⁴ 45 C.F.R. § 164.502(a)(5)(ii)(B)(2).

¹⁵ 45 C.F.R. § 164.510(b)(5).

¹⁶ 45 C.F.R. § 164.522(a)(1)(vi).

¹⁷ 45 C.F.R. § 164.524(c)(2)(ii). The HHS commentary indicates that it expects the information to be produced in machine readable format, such that it can be used on a computer (e.g., Microsoft Word, Excel, text, HTML, pdf). See 78 F.R. 5631.

¹⁸ Section 13405(e) of the HITECH Act; 45 C.F.R. § 164.524(c)(3).

¹⁹ 45 C.F.R. § 164.520(b)(1)(ii)(E).

- An individual's right to restrict PHI disclosure to a health plan where the individual has paid a provider out-of-pocket in full for treatment received.²⁰
- An individual's right to be notified following a breach of unsecured PHI.
- If a health plan CE (excluding an issuer of long-term care policies) intends to use or disclose PHI for underwriting purposes, a statement that the CE is prohibited from using or disclosing Genetic Information for that purpose.

The Final Rule and accompanying HHS commentary also indicate that HHS considers these changes to HIPAA Privacy Notice to be "material." Since the changes are material, health plans must provide the revised notice, or information about the material change and how to obtain the revised notice, to HIPAA-covered individuals. The Final Rule gives health plans two options to comply with this requirement:

1. If the health plan posts its HIPAA Privacy Notice on its website, then the health plan will have to post the revised notice on its website by September 23, 2013. Health plans will then also need to send the revised notice or information about the material change and how to obtain the revised notice in its next "annual mailing" to individuals then covered by the health plan.²¹
2. If the health plan does not post its HIPAA Privacy Notice on its website, then the health plan will need to provide the revised notice within 60 days after the notice was revised.²²

Security Breach

The Omnibus Rule revises the definition of "breach" and removes the "harm trigger" approach adopted in the "interim final" security breach regulation.²³ A breach is now defined as any impermissible use or disclosure of PHI unless it can be shown by a CE or BA that there is a low probability that the PHI has been compromised (or that one of the three exceptions in the original definition applies).²⁴

The Final Rule eliminates the "risk of harm" analysis used in assessing security breaches. Instead, under the Final Rule, there is now a presumption that a breach notification is necessary in all cases, unless a "risk assessment" shows a "low probability" that PHI has been compromised.²⁵

Risk assessment factors: Covered Entities and BAs will need to consider four factors when conducting a risk assessment:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;

²⁰ This is only applicable to health care providers.

²¹ The HHS Commentary gives examples that health plans may provide the revised notices during the beginning of the next plan year or during an open enrollment period. See 78 F.R. 5625.

²² 45 C.F.R. § 164.520(c)(1)(v)(B).

²³ 74 F.R. 42740; See Legislative & Release Information LI-388 for more information.

²⁴ 74 F.R. 42746-42747; See Legislative & Release Information LI-388 for more information.

²⁵ For a discussion of HHS comments on Security Breach, See 78 F.R. 5640-5644.

- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.²⁶

While these factors may have been considered by CEs during past breach investigations, the Omnibus Rule and HHS Commentary emphasize that CEs will need to thoroughly document the consideration of each factor.

Last, there is a small change regarding annual breach notifications to HHS for breaches involving less than 500 individuals. Under the Final Rule, such reports must be made not later than 60 days after the end of the calendar year in which the breaches were “discovered.”²⁷

HIPAA Enforcement Rule and Penalties

The Omnibus Rule adopts the higher penalties for HIPAA violations provided under HITECH.²⁸ There are four categories of violations reflecting increasing culpability and four corresponding tiers of penalty amounts. The minimum penalty amounts are significantly increased for each violation, with **a maximum penalty amount of \$1.5 million annually** for all violations of an identical provision. HHS will not impose the maximum penalty in all cases, but will determine penalty amounts based on the following broad factors:²⁹

- The nature and extent of the harm resulting from the violation;
- The CE’s or BA’s history of prior compliance HIPAA provisions, including any violations;
- The financial condition of the CE or BA; and
- Such other matters as justice may require.

The Final Rule also provides that HHS will investigate all “possible” violations involving willful neglect. The Secretary also has the discretion to commence a “compliance review” instead of an investigation using the same standards of willful neglect by a CE or BA.³⁰

Genetic Information

The Final Rule clarifies that PHI includes “Genetic Information” as defined under GINA. It specifically prohibits use or disclosure of Genetic Information for underwriting purposes by all health plans, except for issuers of long term care policies.³¹ Health plans (except for issuers of long-term care policies) are also required to include a statement in their privacy notices that they are prohibited from using or disclosing genetic information for underwriting purposes.³²

As is currently the case, group health plans are permitted to disclose summary health information to the plan sponsor if the plan sponsor requests the information for: (1) obtaining premium bids; (2) providing health insurance coverage under the group health plan; or (3) modifying, amending, or

²⁶ 45 C.F.R. § 164.402.

²⁷ The prior standard was after a breach had “occurred.” 45 C.F.R. § 164.408(c).

²⁸ Section 13410(d) of the HITECH Act.

²⁹ 45 C.F.R. § 160.408.

³⁰ 45 C.F.R. §§ 160.306; 160.308.

³¹ 45 C.F.R. § 164.502(a); See Legislative & Release Information LI-355 for more information.

³² 45 C.F.R. § 164.520.

terminating the group health plan. The Omnibus Rule, however, clarifies that a group health plan is not allowed to disclose Genetic Information that is prohibited by the underwriting prohibition.³³

Effective and Compliance Dates

The Omnibus Rule becomes effective on March 26, 2013 with a compliance date of September 23, 2013.

In general, while all CEs and BAs will need to comply by the 2013 compliance date, the Final Rule contains a few transition provisions relating to BA agreements and provision of revised HIPAA privacy notices:

- BA Agreements currently in force: CEs will have an additional year (until September 22, 2014) to modify current BA agreements which were in place prior to January 25, 2013.
- HIPAA Privacy Notices posted on a health plan's website: Revised HIPAA privacy notices will need to be posted on the health plan's website by September 23, 2013. Health plans will then need to send the revised notice, or information about the material change and how to obtain the revised notice, in the plan's next "annual mailing" to individuals then covered by the health plan.³⁴

Impact

The Omnibus Rule changes existing rules related to HIPAA privacy and security, breach notification, enforcement, and genetic information disclosure. Covered Entities such as health plans, providers, and health care clearinghouses and their Business Associates will need to review their privacy and security practices, policies, and procedures to ensure they comply with the new Omnibus Rule by the compliance date.

Covered Entities will need to examine their existing BA agreements and HIPAA privacy notices for compliance with these new requirements. BAs will need to review these new HIPAA compliance requirements, particularly in light of their new HIPAA privacy and security obligations, as well as review arrangements with their Subcontractors and enter into new agreements with them as required.

MetLife is aware of the Omnibus Rule's requirements and will be taking appropriate steps to implement them.

³³ 45 C.F.R. § 164.504(f)(1)(ii).

³⁴ Health plans which do not post notices on their website will need to distribute their notices within 60 days after they are revised. See 45 C.F.R. § 164.520(c)(1)(v)(B).