HHS Gets Aggressive: HIPAA Audits & Penalties on the Rise

What You Need to Know

Medical Group Management Association (MGMA)
Racquet Club of Memphis
January 19, 2017

Speaker

Speaker
Jennifer Kiesewetter
Attorney, Kiesewetter Law Firm, PLLC

Jennifer is a seasoned attorney in the field of employee benefits. Her practice includes regulatory compliance and governance with the Employee Retirement Income Security Act of 1974 (ERISA), the Internal Revenue Code and the Affordable Care Act (ACA), in addition to the other federal laws governing employee benefits and health care compliance regulatory law.

901.818.3067 • jkiesewetter@kiesewetterfirm.com

Today's Roadmap

- **Review of HIPAA**
- **Increased Penalties**
- **Recap of 2016: Privacy breaches, hacking, settlements**

Brief Review of HIPAA

HIPAA applies to covered entities and business associates. Both covered entities and business associates must protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

Brief Review of HIPAA

- A covered entity is a health care provider, a health plan, or a health care clearinghouse. Health care providers include providers such as:
  - Doctors
  - Clinics
  - Psychologists
  - Dentists
  - Chiropractors
  - Nursing Homes
  - Pharmacies
- but only if these providers transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

Brief Review of HIPAA

- A health plan includes health insurance companies; HMOs; employer-provided health plans, except for self-administered plans with fewer than fifty (50) participants; and government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs.
- A healthcare clearinghouse includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Brief Review of HIPAA

- If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with HIPAA's requirements to protect the privacy and security of protected health information.
- In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of HIPAA.

Brief Review of HIPAA

- Plan sponsors need to be aware that group health plans, *except for self-administered plans with fewer than fifty (50) participants*, are covered entities under HIPAA.
- Further, although a group health plan must comply with HIPAA, compliance is limited for fully-insured group health plans.
- A group health plan is a separate legal entity from the employer and any other parties who sponsor the group health plan.
- As such, neither the employer nor the plan sponsor is a covered entity under HIPAA.

Brief Review of HIPAA

- Because only the group health plan is a covered entity under HIPAA, only the group health plan itself is subject to the rules, and the penalties, of HIPAA.
- However, HIPAA's Privacy Rules control the conditions under which the group health plan can share protected health information with the employer and the plan sponsor when the information is necessary for the employer or the plan sponsor to perform certain administrative functions on behalf of such group health plan.
- For example, HIPAA requires, under these circumstances, that a receipt of certification from the employer or plan sponsor that the health information will be protected as prescribed by HIPAA and will not be used for employment-related actions.

New Regulations: Increased Penalties

- On November 2, 2015, Congress enacted the Federal Civil Monetary Penalties Inflation Adjustment Act of 2015, which required federal agencies to make "catch-up" inflation adjustments.
- The catch-up increases would be effective for any penalties assessed after August 1, 2016.

New Regulations: Increased Penalties

- This catch-up adjustment applies to HIPAA penalties.
- HIPAA penalties have not been adjusted since 2009.

New Regulations: Increased Penalties

- On September 2, 2016, the Department of Health and Human Services (HHS) issued interim final regulations that adjust the civil monetary penalties that fall under HHS's jurisdiction, including HIPAA penalties.
- Because the 2015 Act stated that the catch-up adjustments must be effective no later than August 2, 2016, these regulations were released for *immediate implementation with no comment period and no notice that normally accompanies most regulations.*

New Regulations: Increased Penalties

- The HIPAA penalties specifically focus on the Administrative Simplification requirements, which are part of HIPAA.
- The Administrative Simplification provisions of HIPAA require the HHS to adopt national standards and operating rules for electronic health care transactions, code sets, national identifiers, and other administrative aspects of health care delivery.
- HIPAA Administrative Simplification requirements apply to all HIPAA-covered entities; i.e., health plans, clearinghouses, and health care providers who conduct electronic health care transactions.

New Regulations: Increased Penalties

DESCRIPTION	CURRENT PENALTY	UPDATED PENALTY
Violation pre-HITECH	$100 per violation $37,561 annual cap	$150 per violation $37,561 annual cap
Violation w/o knowledge	$100 minimum $50,000 maximum $1.5 million annual cap	$110 minimum $55,010 maximum $1,650,300 annual cap
Violation w/ reasonable cause AND NOT due to willful neglect	$1,000 minimum $50,000 maximum $1.5 million annual cap	$1,100 minimum $55,010 maximum $1,650,300 annual cap
Violation due to willful neglect AND corrected w/in 30-day period	$10,000 minimum $50,000 maximum $1.5 million annual cap	$11,002 minimum $55,010 maximum $1,650,300 annual cap
Violation due to willful neglect AND NOT corrected during 30-day period	$50,000 minimum $1.5 million maximum $1.5 million annual cap	$55,010 minimum $1.65 million maximum $1.65 million annual cap maximum

HHS Activity

- HHS has become more aggressive with audits, and with increased penalties, employers simply cannot afford an audit on HIPAA rules and regulations.
- In August 2016, HHS announced that it would begin broader investigative efforts with respect to breaches affecting *fewer than* 500 individuals.

HHS Activity

- In 2016, the Office for Civil Rights (OCR) at HHS (which enforces HIPAA), recorded **$23.5 million in payouts** for HIPAA violations as enforcers are unable to settle.
- This was four times over the previous record high set in 2014 of $7.9 million.
- FYI: 2015 was $6.19 million.

HHS Activity

- Average payouts also increased:
  - **2016: $1.81 million**
  - 2015: $1.03 million
  - 2014: $1.32 million
  - 2013: $0.75 million
  - 2012: $0.97 million

HHS Activity

- In our own backyard, in 2016, the University of Mississippi Medical Center sustained a $2.75 million penalty stemming from an HHS investigation into a relatively small 2013 HIPAA breach involving a stolen laptop.
- However, during the course of the investigation, serious HIPAA security and privacy issues were uncovered, resulting in the $2.75 million penalty.

HHS Activity

- Other HHS Activity Facts and Figures from 2016:
  - The number of large breaches (over 500 affected) was the highest to date, ringing in at 313 (over the previous highest of 307 in 2014).
  - 16 million patient records were potentially compromised due to HIPAA breach, ringing in at the second highest (highest was 113 million in 2015).
  - Top causes of breach:
    - Unauthorized Access / Disclosure (41%)
    - Hacking / IT Incidents (33%)
    - Theft (19%)
    - Loss (5%)
    - Improper Disposal (2%)

HHS Activity

- ***Who is being targeted?***
  - Health care providers – 79% of breach targets (highest on record)
    - 72% in 2015
    - 59% in 2014
    - 67% in 2013
  - Health plans – 14% of breach targets (second highest on record)
    - 23% in 2015
    - 12% in 2014
    - 7% in 2013
  - Business Associates – 6% of breach targets
    - 4% in 2015
    - 22% in 2014
    - 21% in 2013

Questions & Answers

Jennifer S. Kiesewetter, Esq.
Kiesewetter Law Firm, PLLC
1661 International Place Drive, Suite 400
Memphis, TN 38120
901.818.3067
jkiesewetter@kiesewetterfirm.com
www.kiesewetterfirm.com