News

"Sorry" Just Won't Cut It Any More: HIPAA Data Breaches Bring Serious Legal Consequences

Howard Fienberg, MRA Director of Government Affairs
September 22, 2009

New additions to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules by the stimulus law earlier this year dramatically alter the legal requirements for research organizations ("business associates") handling "protected health information" (PHI) for healthcare entities such as hospitals and insurance companies ("covered entities"). While the rules used to only impact business associates in their contracts with covered entities, the stimulus law provisions (known as the HITECH Act) apply those rules directly to business associates, imposing heaps of new liability. We will look at those rules in depth later. For now, let us discuss the regulations coming into effect on September 23 on data security breach notification.

The security breach regulations, coming into effect this month, require HIPAA covered entities to promptly notify affected individuals of a breach of their unsecured PHI, as well as the Secretary of Health & Human Services (HHS) and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals have to be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

The rules apply to all breaches occurring on or after September 23, 2009 that are discovered by covered entities and business associates. However, there is a little bit of breathing room: the HHS Interim Final Rule indicates that HHS will not impose sanctions for failure to notify with respect to breaches that are discovered within the first 180 days after the effective date. Enforcement starts on February 22, 2010.

The FTC and Personal Health Records

In concert, the Federal Trade Commission (FTC) issued a Final Rule on breach notification for "personal health records" (PHRs) – the new electronic health records being promoted by the HITECH Act. It applies to all breaches discovered on or after September 24, 2009 by "foreign and domestic vendors of personal health records, PHR related entities, and third party service providers" that "maintain information of U.S. citizens or residents." Researchers could conceivably qualify as "third party service providers" and would have to notify the PHR vendor, or PHR related entities to which they provide services of any breaches they discover.

Unlike the HHS rule, the FTC presumes a reportable breach occurred unless the entity can provide "reliable evidence" that the PHR data wasn't or couldn't reasonably have been subject to unauthorized access. Also, the FTC rule only applies to electronic data, while HHS' rule applies to both electronic and paper data.

CMOR will provide further guidance as necessary.

Defining a Breach: the Clock Starts Ticking

Covered entities have 60 days from first discovering a breach (or from when they should have reasonably known if exercising reasonable diligence) within which they must notify any individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or

disclosed in a manner that compromises its security or privacy. Depending on the severity of the threat, covered entities may be required to provide notice much sooner.

Business associates must notify their covered entities about breaches – and the clock may start ticking once a business associate discovers a breach just as it would if the covered entity did (depending upon whether or not the business associate is considered an "agent" by the law). That means that covered entities will likely be revising their business associate contacts to require rapid and rigid reporting. However, the business associate does not need to provide full identification of individuals subject to a breach, just "to the extent possible."

Thankfully, HHS decided upon a harm threshold, whereby a breach requires the risk of significant harm (financial, reputational or otherwise) to the affected individual.

There are also a few exceptions to the definition of a "breach":

- Where an employee or agent of a covered entity or business associate accidentally acquires, accesses or uses unsecured PHI (as long as it is made with good faith and the employee or agent ensures that the data will no longer be subject to unauthorized use or disclosure);
- Inadvertent disclosure of unsecured PHI by an authorized employee or agent of a covered entity or business associate to a similar individual elsewhere in the same organization, but there is no further unauthorized use or disclosure;
- Where unsecured PHI is disclosed to an unauthorized person, but the covered entity or business associate believes in good faith that the recipient would not reasonably have been able to retain the PHI; and
- Where the unsecured PHI has been stripped of 16 direct identifiers (leaving it a "limited data set"), dates of birth, and zip codes.

Encrypt or Destroy – Safe Harbor

The HHS and FTC rules apply only to "unsecured" PHI. They have provided an important exemption from the breach notification requirements for data that has been encrypted or destroyed. CMOR recommends all research organizations implement encryption and destruction protocols for any and all data, not just PHI, because this exemption is likely to be the national standard for any data once Congress agrees to a federal data breach law.

Violations Will Cost You Dearly

Violating these and other HIPAA rules will bring hefty penalties. The HITECH Act:

- Raises the maximum fines for rule violations from $25,000 to as much as $1.5 million, and subjects "willful neglect" to mandatory maximum fines;
- Opens violations to enforcement by state Attorneys General; and
- Allows enforcement against individuals employed by covered entities.

More to Come

CMOR will provide further information on business associates' new responsibilities under the amended HIPAA Privacy and Security rules soon, in MRA publications and in the Compliance Guide.

Resources

- Interim Final HHS Breach Notification Rule (74 CFR 42740): http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf
- FTC standard form: "Notice of Breach of Health Information": http://www.ftc.gov/os/2009/08/R911002hbnform.pdf
- FTC Final Rule: http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf
- The Compliance Guide: http://www.mra-net.org/ga/dref

Disclaimer: The information provided in this article is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. MRA advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.