What You Need To Know About The HIPAA Mega-Rule

By William H. Maruca

The long-overdue HIPAA/HITECH "Mega-Rule" has finally arrived. The Department of Health and Human Services published the Omnibus Rule in the January 25, 2013 Federal Register after missing several predictions of its imminent release. The four-part rule modified the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, adopted changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, finalized the rule for breach notification of unsecured protected health information (PHI); and implemented the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes. The final rule takes effect on March 26, 2013, but healthcare providers and other covered entities (and their business associates) generally have until September 23, 2013 to modify their policies and meet new requirements. Some of the more relevant features of the omnibus rule include:

Business associates will now be directly liable for compliance with the HIPAA Privacy and Security Rules. Further, more entities will be defined as business associates, including companies that maintain PHI, such as storage facilities and cloud computing/data storage vendors (but not those that only transmit the PHI and do not regularly access the content of the PHI, such as telecommunications providers or couriers). Additionally, business associates' subcontractors will be treated as business associates themselves, subject to primary liability exposure. Business Associate Agreements must be updated by September 23, 2013 except where valid agreements were in place on July 25, 2013, in which case the deadline may be extended up to an additional year.

Use of PHI for marketing and fundraising purposes is restricted and individuals must be given the opportunity to opt out. The sale of protected health information without individual authorization is prohibited.

Individuals have the right to prevent disclosure of records of any treatments they have personally paid for. Some individuals choose to pay out-of-pocket for care that they consider potentially embarrassing or compromising, such as mental health or drug and alcohol treatment, and they will be able to prevent the further release of any information regarding such care.

Unauthorized disclosures of PHI will be presumed to be reportable breaches unless the covered entity can show that there is a low probability that the protected health information has been compromised..

A minimum of four factors must be taken into account and documented when determining whether a disclosure is a reportable breach: the nature and extent of the disclosed information; the person to whom the disclosure was made; whether the information was actually acquired or viewed; and the extent to which risk to the information has been mitigated.

For example, a single fax containing only a patient's name and address that is mistakenly sent to the wrong physician, when that physician is immediately notified and agrees to destroy or return the fax, may present a low probability that the information has been compromised. By contrast, a lost laptop containing unencrypted patient data including birthdates, social security numbers and diagnoses, where the covered entity cannot determine who has found the laptop or whether anyone has seen the data, would represent a much greater risk of compromise. Remember that data encrypted in accordance with the standards of the National Institute of Standards and Technology (NIST) is generally not considered "breached" when inadvertently disclosed, such as when devices containing such data are lost or stolen. Too many covered entities and business associates have failed to implement encryption policies that could have prevented disaster.

Covered entities should act soon to work with knowledgeable counsel to take necessary steps to comply with the omnibus rule, including:

Identify all business associates including those newly designated under the new rule; review and update business associate agreements;

Review, update and redistribute your Notice of Privacy Practices;

Review and revise your breach analysis and notification policies and procedures;

Review your security policies, particularly with regard to mobile devices and "bring-your-own-device" technology, and implement NIST-compliant encryption wherever possible.

As recent high-profile enforcement actions have indicated, the risks for ignoring your HIPAA/HITECH responsibilities can be catastrophic, and the highest penalties apply in cases of "willful neglect."

William H. Maruca is a partner with the Pittsburgh office of the law firm of Fox Rothschild LLP who concentrates his practice in healthcare. He can be reached at wmaruca@foxrothschild.com or 412.394.5575.