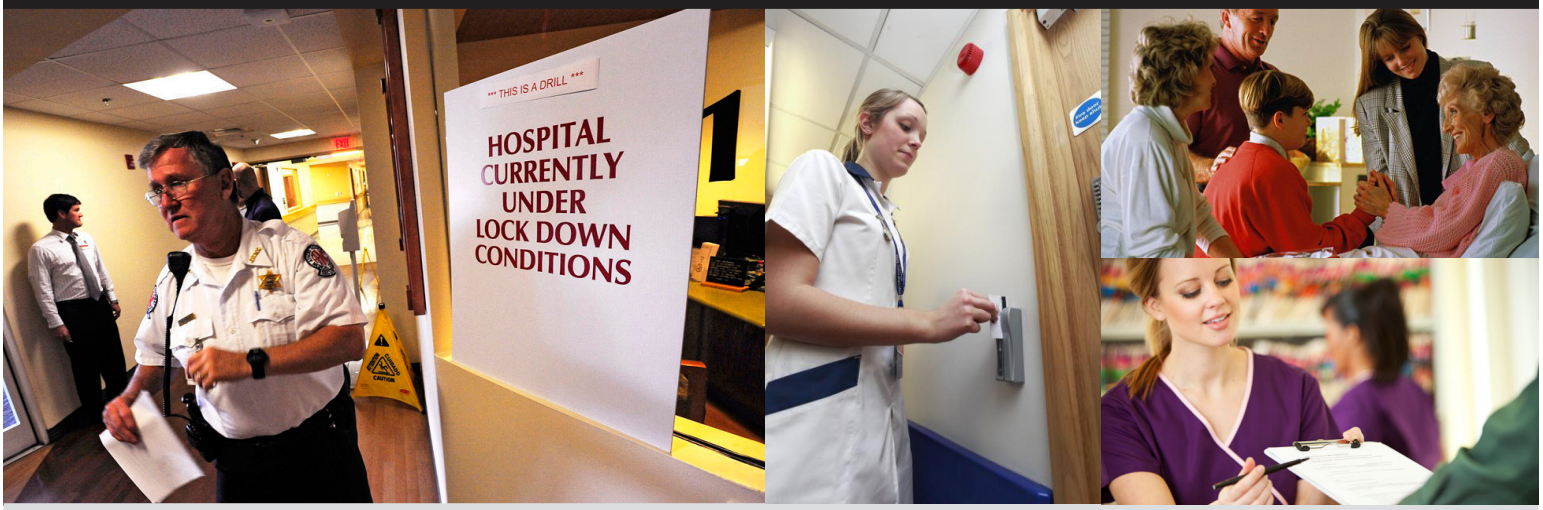
RiskWatch

www.riskwatch.com



HIPAA Omnibus & HITECH Rules:

Key Provisions and a Simple Checklist

Introduction

Last year, the federal government published its long awaited final regulations implementing the "Health Information Technology for Economic and Clinical Health (HITECH) Act. In general, the new rules expand the obligations of physicians and other health care providers to protect patients' protected health information (PHI), extend these obligations to a host of other individuals and companies who, as "business associates," have access to PHI, and increase the penalties for violations of any of these obligations. In announcing these changes HHS Office for Civil Rights Director Leon Rodriguez said, "These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

The Summary of the Modifications are:

- Requires Business Associates of Covered Entities directly responsible for compliance with certain of the HIPAA Privacy and Security Rules' requirements. A Business Associate is any company that sends or routinely accesses patient health information. These groups could be health IT companies, e-prescribing gateways; vendors of personal health records. It also includes subcontractors who create, receive, maintain or transmit protected health information for business associates.
- Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
- Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
- Require modifications to, and redistribution of, a Covered Entity's notice of privacy practices.
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

What the Provisions Means to You?

- The new rule underscores providers obligation to give patients access to their medical records in the electronic format they prefer. That means that despite the sensitivity over data security, the patient can request that the data not be in an encrypted format. McGraw added that the hospital need only notify the patient of the security risk if the data isn't encrypted.

- Before a provider markets a third party service to patients based on their PHI, or to sell or provide access to PHI for payment, the provider must request permission to do so from each patient who's PHI it wishes to use. Business agreements that were in place before January this year have a one year extension — they need to be updated by September 23, 2014.

- Any parts of your organization that act like covered entities need to comply with HIPAA, and any parts of your organization that provide services and support to those business units, and also access PHI, will likewise need to comply with HIPAA.

- Incidents that violate the Privacy Rule that do not meet one of the provided exceptions, and that are not subject to a safe harbor (see below) are presumed to be breaches. To defeat that presumption, covered entities and business associations must evaluate the incident using the risk analysis approach outlined by the final rules. Notification will be required if the risk analysis reveals there is greater than a "low probability" that the PHI will be or has been compromised.

- The risk analysis now required by the final rules must be documented and retained to meet the covered entity's burden of proof to demonstrate that unreported incidents did not rise to the level of a "breach."

- Business associates will need to bring their subcontractors into the loop by asking them to execute appropriate HIPAA contracts (a.k.a., business associate agreements). While that should have occurred under current rules, the requirement is not explicit. Motivation to do so should be high since business associates can now be held directly liable for any failure in this regard.

- As was already the case, business associates must report security breaches to covered entities, and covered entities are required to report breaches to affected individuals and HHS

- There will be many more compliance reviews and complaint investigations. Since the agency always requests copies of HIPAA policies in these reviews, it's definitely time to update your policy book.

- Following a complaint, a reported breach, or similar incident, the agency may conduct an inquiry with the covered entity or business associate to gather additional facts to assess whether willful neglect or some greater culpability caused the violation. If so, the agency will be strictly required to conduct a compliance review.

- Expect to see more formal investigations and settlement orders since informal resolution is no longer mandatory.

Fines and Penalties

Degree of Culpability / "State of Mind"	Potential Penalty Per Violation	Maximun Annual Cap for All Violations of Identical HIPAA Provision
Violation was not known and could not have been discovered with reasonable diligence	$100 – $50,000	$1,500,000
Reasonable cause for violation, not due to willful neglect	$1,000 – $50,000	$1,500,000
Violation due to willful neglect, but corrected in 30 days	$10,000 – $50,000	$1,500,000
Violation due to willful neglect, **not** corrected in 30 days	$50,000	$1,500,000

- HHS provides that covered entities are permitted to send individuals unencrypted emails including ePHI if the individual requests it, provided the covered entity has advised the individual of the risk and the individual still prefers to receive the message by unencrypted email."

- Covered entities should ensure that business associates comply with the Security Rule and other applicable portions of these rules that now apply directly to them. That increased vigilance is advisable not only because covered entities can be directly liable for business associate noncompliance, but also due to enhanced breach notification requirements (covered entities must report breaches caused by business associates unless they contract otherwise) and the agency's enhanced fining authority. Business associates should undertake Security Rule implementation now and redouble any existing efforts to comply prior to the September 23, 2013 compliance deadline

- Business associates will need to execute compliant business associate agreements with their subcontractors, and can expect to see their covered entity clients pushing out tougher business associate agreements that will seek liability protections such as indemnification.

Checklist

For Covered Entities

1. Update Notice of Privacy Practices and post on website

2. Update Patient Authorization Form

3. Update privacy policies, including the following:
   - Uses and Disclosures of Patient Information to include reference to genetic information, sale of protected
   - health information, restriction on disclosure of information to health plan if the service is paid in full by
   - patient and disclosure of patients' records deceased over a 50-year period
   - Use and Disclosure of Protected Health Information for Marketing Activities
   - Use and Disclosure of Protected Health Information for Fundraising Activities

4. Implement a process for requests to disclose immunization records to schools as required by law

5. Prepare Authorization Form for disclosure of immunization records to schools

6. Implement a form for Patient Requests to Restrict Disclosure of Protected Health Information to a Health Plan

7. Update Patient Record Request form to include the option of providing an electronic copy to patient

8. Update list of business associates and amend Business Associate Agreements

9. Update Breach Notification Compliance Plan

10. Ensure there is a process for confirming that business associates have entered into written contracts with subcontractors and vendors and that the subcontractors' policies and procedures are HIPAA compliant

For Business Associates

1. Implement privacy policies:
   - Uses and Disclosures of Patient Information
   - Patient Access to Health Information
   - Accounting of Disclosures
   - Amendment of PHI
   - Confidentiality and Non-disclosure Agreement

2. Implement Security Policies. The following Security Policies are required by the Security Rule:
   - Information Security Risk Analysis Policy
   - Information Security Risk Management Policy