3 Major changes in HIPAA regulations covered entities & business associates should know

By Bruce 'Andy' Andrews • Thursday, September 12, 2013

Last time we shared practical steps that Covered Entities (“CEs”) and Business Associates (“BAs”) should take now to comply with the HIPAA Mega-Rule, as issued by the U.S. Department of Health & Human Services, Office of Civil Rights (“OCR”). The compliance deadline for these changes is no later than September 23, 2013. Below we discuss in detail the major changes related to Notice of Privacy Practices; HIPAA policies and procedures; direct liability for BAs; and the expanded BA definition.

1. **Notice of Privacy Practices (“NPP”).** CEs must update their NPPs. In addition to the requirements regarding the use and disclosure of PHI, the updated NPP should include the following:

   - **Additional Statements.** A statement that certain uses or disclosures of PHI require an authorization, including for potential fundraising or marketing purposes, the sale of PHI, most disclosures of psychotherapy notes and others.
   - **Fundraising Opt-Out.** If a CE will use or disclose PHI for purposes of fundraising, the NPP must include a statement that the CE may contact the individual for purposes of fundraising, and must also include a statement that the individual has a right to opt out of any fundraising.
   - **Breach Notification.** The updated NPP must inform individuals of the right to be notified following a breach involving the individual's unsecured PHI.
   - **Restriction for Providers.** The updated NPP must inform an individual that they have a right to restrict disclosures of their PHI by a provider to a health plan, if the individual pays for the services in full, out-of-pocket, and requests that the provider not disclose PHI related to those services.
   - **Genetic Information Nondiscrimination Act (“GINA”).** For health plans, the updated NPP must state that the health plan generally may not use or disclose genetic information for underwriting purposes.
   - **Distribution of NPP.** The required changes to NPPs are considered a “material revision.” CEs must redistribute revised NPPs in accordance with the current HIPAA requirements. A health care provider must have the revised NPP available where they perform health care services, and post the revised NPP in a clear and prominent location. Health care providers must give a copy of the revised NPP to new patients and make a good faith effort to obtain an acknowledgment of receipt. Existing patients must be given a revised NPP upon request. If the CE is a health plan, the revised notice must be posted on the website and distributed with the next annual mailing. If the health plan does not maintain a website, it must provide the revised NPP or information about it to individuals covered by the plan within 60 days of revision.

2. **Business Associates, Covered Entities, Policies & Procedures.** Before HITECH, BAs were obligated to comply with HIPAA via the terms and conditions of their Business Associate Agreement with a CE. Now, like CEs, BAs must directly comply with the law and are subject to severe civil monetary penalties (“CMP”) for HIPAA violations. The government will now hold a BA directly liable for its violation of the privacy and security rules, and a BA has potential liability for its subcontractors’ violations, as well. Given the potential liability, both CEs and BAs should have appropriate policies, procedures, and safeguards in place to address the HIPAA Privacy and Security rules and should only contract with those parties demonstrating the same level of commitment to privacy and security compliance.

   - **Who Qualifies as a BA?** Whether a person or entity is a “business associate” is a functional test – it is based on what a person or entity does for the CE. A person or entity may be a BA even without intending to be.
   - **A BA is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI either on behalf of a CE, or in providing services to a CE, other than as a member of the CE’s workforce.**
   - **BA functions and activities include claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.**
   - **BA services include legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.**

Policy & Procedure Manual. Adopting a policy & procedure manual is an important step for a CE or BA to comply with its obligations under HIPAA and HITECH. CEs and BAs must review and adopt policy & procedure manuals, and ensure that employees are properly trained to follow the policies and procedures to protect PHI and implement proper security precautions.
3. **Updating Business Associate Agreements.** All BAs now must comply with physical, technical and administrative safeguards, adopt policies & procedures and meet certain documentation requirements.

- **Reporting.** BA agreements must require BAs to report breaches of unsecured PHI to the CE.

- **Privacy Obligations.** Where a BA agreement delegates Privacy Rule obligations to the BA, the BA must comply with those obligations in the same manner and to the same extent as would the CE or an "upstream" BA.

- **Security Rule.** BA agreements must require that the BA complies with the Security Rule relating to electronic PHI.

- **Satisfactory Assurances.** BAs must obtain satisfactory assurances from subcontractors that the subcontractor will safeguard PHI. An example of satisfactory assurances would include a properly executed BA agreement with the subcontractor.

- **Grandfathered BA Agreements.** Under the Mega-Rule, certain BA agreements may be grandfathered for one year. To be grandfathered, however, an existing BA Agreement must (a) have been entered into prior to January 23, 2013; (b) be in compliance with the HIPAA rules at the time; and (c) not renewed or modified between March 25, 2013 and September 23, 2013.

In addition to the practical steps outlined above, CEs and BAs should be aware of other substantive changes included as a part of the Mega-Rule, including new rules regarding access to PHI, limits on the use of PHI, breaches and notification, enforcement, and penalty structure. We will discuss these additional major changes in our next post.

For more information, please contact:
Bruce 'Andy' Andrews
bandrews@sirote.com
205.930.5757