FOCUS...on the North Florida Chapter

North Florida Chapter

ACC Association of Corporate Counsel NORTH FLORIDA

2015 4th Quarter Newsletter

Patrolling Cyberspace: Corporate Counsel's Role in Assuring Sufficiency of "Business Associate" Agreements Under HIPAA

By Susan E. Mack, Esq. (Adams and Reese LLP)

1. Corporate Counsel's Responsibilities Under Updated Rules related to the Health Insurance Portability and Accountability Act of 1996

While the Health Insurance Portability and Accountability Act of 1996 (HIPAA) did not originally contain strictures governing the privacy of health information, related privacy rules now grapple with the real risks posed by electronic transmission of health data. Originally enacted by the Department of Health and Human Services in 2000 and 2002, but amended as recently as last year, these privacy rules acknowledge an individual's right to maintain the confidentiality of his or her identifiable health information.(i) These mandates take into consideration the harm that could be caused if this sensitive information is disseminated by hacking into a computer network or through access by an unauthorized user to such a network-- as well as by such low-tech means as the theft of documents containing the data.

What needs to be protected? Protected Health Information or "PHI" consists of all "individually identifiable health information that is (a) transmitted by electronic media; (b) maintained in electronic media or (c) transmitted in any other form or medium."(ii)

Who needs to be concerned with whether PHI is adequately safeguarded? Among those who should be charged with patrolling cyberspace are all corporate counsel employed by "covered entities"; namely, health care providers, health plans and health care clearing houses.(iii) The standard that must be observed by these entities and their counsel is the requirement to keep disclosure to the "minimum necessary" to achieve appropriate aims in using the data.(iv) And it is not just the workforce of the covered entities themselves that is charged with such compliance. The covered entity's corporate counsel should check that his or her employer is absolutely receiving "reasonable assurances" that its "business associates" such as retained law firms, claims processors, actuarial firms, accounting firms and consultants all appropriately protect PHI.(v)

A "business associate" is defined as any individual or entity which creates, receives, maintains or transmits PHI.(vi) To clarify, a business associate is not an employee of a covered entity, but it is true that a covered entity may be a business associate of another covered entity. Permissible purposes for a business associate's use of PHI can include claims processing or administration, data analysis or administration, data analysis, and data aggregation, among other functions.

2. What Leads to Heightened Concerns Today, both on part of Business Associates and Covered Entities?

Today the substance of HIPAA rule restrictions apply to business associates just as they do to covered entities. Business associates were formerly liable to covered entities only for breach of contracts in effect with the entities, but now they are directly liable for wrongful use or dissemination of PHI.(vii) Furthermore, certain business associate duties are heightened. For example, a covered entity now maintains no direct liability for a business associate's subcontractor; rather, the business associate is responsible for its subcontractors' wrongful dissemination of information. (viii)

Let's move to the real life ramifications of business associates' enhanced accountability. The Office of Civil Rights, the administrative body responsible for enforcing these rules, is empowered to perform (a) audits of each of covered entities, business associates and their

subcontractors and (b) investigations of reported violations. If resulting findings are adverse, covered entities or business associates can be assessed civil monetary fines of $50,000 per individual record, up to an aggregate total of $1.5 million per calendar year.(ix) Criminal penalties can be imposed for knowing violations.(x)

For a covered entity's corporate counsel, the specter of damage that can be done by a non-compliant business associate is just as daunting as the prospect of monetary damages. At the eighth annual conference entitled "Safeguarding Health Information: Building Assurance Through HIPAA Security" held in September 2015(xi), risks associated with business associates were identified as one of the Office of Civil Rights top three investigative priorities for 2016. To date, 179,000 incidents of authorized exposure of PHI have occurred from all sources, with approximately 500 individuals affected. It was reported that several recent large breaches emanated from business associates who, typically, possess even more data than covered entities.

3. Keeping the Business Associate Contract Tight-What to do about the Enhanced Risk!

How does a covered entity's corporate counsel obtain reasonable assurances from a business associate, given these looming risks? The regulatory mandate dictates that such assurances are achieved by means of a written agreement with the business associate (and the business associate must do the same for its subcontractor)(xii). Helpfully, the regulations set forth the requisite elements of the contract(xiii); but, pragmatically speaking, there are several drafting tips that will result in an understandable and workable agreement.

First, the agreement should set forth its purpose that compliance is intended not only with HIPAA, but with the subsequent HITECH Act of 2009. To make sure the scope of the business associate agreement keeps pace with changing future regulation, it is best to also include reference to "any implementing regulations that "have been or may be adopted." The far-sighted drafter of the agreement should also reference intended compliance with state statutes that may be more restrictive than the federal regulatory schematic.

Second, to provide necessary context, the agreement should contain an acknowledgement that there is a business relationship in place by which the business associate performs certain functions or activities which have or will involve the creation, receipt, maintenance or transmission of PHI. If there is already a services contract in place which describes these functions (such as a third party administration contract, as an example), that contract should be specifically referenced.

Third, the agreement must state the required and permitted uses and disclosures of PHI. These uses include those functions necessary for the management of the business associate itself, but obviously should not include any uses prohibited by the privacy rules.

The tone of the agreement should make clear the obligation that the disclosures are only those narrowly tailored to effect the good faith purposes of the business associate. To that end, the agreement must state that disclosures are either required by law or that the business associate itself obtains reasonable assurances from all persons to whom disclosure is made that the information will remain confidential, excepting for purposes for which it was disclosed or as required by law. Interestingly, in this context, "as required by law" means a court order, rather than a subpoena that may be signed by an attorney.

Requisite stated disclosures include the duty to disclose to the individual who is the subject of the PHI. Accordingly, that individual is entitled to an accounting of the disclosures of his or her PHI, as well as to the opportunity to amend the business associate's records, presuming the individual finds them to be inaccurate.

Fourth, the agreement must make clear those safeguards which the business associate will employ to keep PHI confidential. A sound drafting strategy is to set forth the basic premise that the business associate will comply with all requirements of HIPAA, the HITECH Act, implementing regulations and applicable state law, but then proceed to set forth a recital of select elements illustrative of the statutory and regulatory requirements. Key among these is not only the duty to maintain internal records as to maintenance of PHI, but to make such available to the covered entity, at its request, and also any investigative authorities such as the Office of Civil Rights and Department of Health and Human Services.

Fifth, the business associate has an affirmative duty to notify of breach of the agreement's protections.(xiv) The agreement should make clear that the business associate will provide a written report of the breach to the covered entity's privacy officer as soon as reasonably possible (a good practical guideline is within three days), and to conduct an immediate investigation to determine what happened, a description of what was disclosed as well as a corrective action plan to mitigate the harmful effects of the disclosure.

Sixth and last, as any contract does, this agreement must address its own termination. The agreement must specify that, in the event of the business associate's violation of a material term of the agreement, the covered entity may terminate the agreement. In the event of any termination, whether for cause or because the business relationship has ceased, the agreement shall either (a) mandate that protections survive agreement termination (if destruction of records is impracticable) or (b) actually mandate destruction of the records containing PHI. Care should be taken to make sure there is no inadvertent retention of PHI- i.e., media (such as hard drives) should be wiped clean once the business relationship comes to a close.

---

i. 65 Fed. Reg. 82462 (Dec. 28, 2000); 67 Fed. Ref. 53181 (Aug. 14, 2002); 45 C.F. R. Parts 160 and 164

ii. 42 U.S. C. Section 1320 (d) (6); 45 C. F.R. 160.103

iii. 45 C.F. R. 160.103

iv. 45 C.F.R. Section 164.502 (b) (1)

v. "Not So Hip? The Expanded Burdens and Consequences to Law Firms as Business Associates under HITECH Modifications to HIPAA", 13 Rich. J. L. +Pub. Int. 313, 321-322

vi. 45 C. F.R. Section 160.103

vii. In 2009, passage of the HITECH (Health Information Technology for Economic and Clinical Health) Act as part of the American Recovery and Reinvestment Act imposed new privacy and security requirements on covered entities and business associates alike. Business associate liability was further clarified via omnibus regulations passed in 2013. See 78 Fed. Reg. 5570, 5597 (Jan. 25, 2013)

viii. 45 C. F. R. Section 164.308(b) (1)

xi. Pub. L. 111-5 (Feb. 17, 2009); Section 13410; 45 C. F.R Section 160.404(b)

x. Department of Health and Human Resources website, "Health Information Privacy" (Dec. 2015)

xi. 20 No. 9 Cyberlawyer NL 5 (October 2015)

xii. 45 C. F. R. Sections 164.308 and 164.314(a)

xiii. 45 C. F. R. Sections 164.502(a)(3) and 164.504(e)(2)

xiv. 45 C.F. R. Section 164.410

Susan E. Mack serves as Special Counsel with the Jacksonville office of law firm of Adams and Reese LLP, following her 25 year career as General Counsel and Chief Compliance Officer of both insurance companies and reinsurers in the life/health and property/casualty sectors of the insurance industry. Adams and Reese LLP, an AmJur 200 law firm, has 280 lawyers in seven Southern states and the District of Columbia.

While working as Senior Vice President and General Counsel of The Main Street America Group, Ms. Mack was one of the co-founders of the ACC North Florida Chapter. From 2010-2011, she had the privilege of serving as the ACC North Florida Chapter's President. During her tenure, the chapter secured the "Best Small Chapter of the Year" award from the ACC national organization.