12-2011

HIPAA Compliance Resources

Paul M. Birch
University of Richmond, pbirch@richmond.edu

HIPAA Compliance Resources

by Paul Birch

As health care consumers, attorneys may need no introduction to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] It may have introduced itself to you already in the form of a refused request for your spouse's pharmacy receipts without signed authorization, or lengthier patient information forms to fill out before seeing a new doctor. On the other hand, the legislation may have facilitated your own access to your personal health records that otherwise would have been denied, or shielded those records from public disclosure by deterring a mass data spill. Along with establishing portability requirements for employee health plans and standardized coding for health transactions—and several other health care-related topics beyond the scope of this article—the agency rules mandated by HIPPA set the standards for privacy and security of health information stored or transmitted by covered entities. Here are some starting points for HIPAA compliance research.

Primary Law

As originally enacted, HIPAA created civil and criminal penalties for wrongful disclosure of individually identifiable health information,[2] but did not establish privacy standards. However, the statute contemplated Congress doing so in separate legislation within 36 months of HIPAA's passage, delegating rule-making authority to the secretary of Health and Human Services only if Congress did not meet that deadline. The deadline passed without any such legislation.

The resulting HHS rules, codified at 45 C.F.R. Part 164, comprise a two-pronged regulatory scheme:

> Security Standards,[3] defining administrative, physical, technical, and organizational safeguards for covered entities' handling of electronic health information.
>
> Privacy Standards,[4] defining the covered health care entities and the uses requiring or not requiring patient authorization. Also included are provisions requiring and specifying the form of notification of privacy policies and asserting a patient's right to request enhanced privacy.

HIPAA enforcement rules and procedures can be found at 45 C.F.R. Part 160. Administrative enforcement is handled by HHS's Office for Civil Rights.

Newer federal legislation, the Health Information Technology for Economic and Clinical Health (HITECH) Act,[5] part of the American Recovery and Reinvestment Act of 2009, amended HIPAA by extending liabilities to "business associates" of covered entities and enhances breach notification requirements. HITECH also expanded HIPAA violation penalties substantially and required HHS to issue annual guidance to the industry as to effective and appropriate security, particularly in the area of data encryption.[6] Predictably, these recommendations have already found their way into security regulation revisions.

The attorney is urged not to overlook Virginia's Patient Health Records Privacy Act,[7] essentially the state's "little HIPAA." Most notably, Virginia offers patients the private right of action for health privacy violations that HIPAA does not.[8]

Compliance Resources

The rapidity of HHS rule changes, especially in light of the HITECH legislation and regulations, render less useful the handful of pre-2010 print HIPAA compliance manuals lacking supplementation, except, perhaps for the broadest of overviews. One would expect, however, a crop of new titles of this kind in the coming years. Indeed, among print resources, one of the few of current value is the American Health Lawyers Association's looseleaf *Health Law Practice Guide*, published by Thompson Reuters/West. The guide devotes a chapter each to HIPAA and HITECH, and includes a number of relevant forms and practice checklists in its appendices.

Among Internet resources, a likely first stop is HSS's own Health Information Privacy website.[9] Designed for patients, health care workers, and attorneys, the site includes concise lay-oriented explanations of the privacy and security rules, complaint forms, and training materials for covered health care entities. It also reproduces the statute and regulations, along with HHS news releases.

It was not until this year that DHS levied its first HIPAA fine against a provider — a $4.2 million fine against Cignet Health — signaling to the industry the potential for huge liability exposure.[10] As such, a growth industry of websites has lately emerged, dedicated to providing compliance guidance by combining free information with offers to sell commercial products or services such as record tracking software and staff training courses. The number of hits generated by entering "HIPAA compliance" in a search engine may surprise you; the range of quality and quantity of information offered on the free side may be less surprising. One can usually recognize these sites by the presence of the HIPAA acronym somewhere in their address.

Of particular note are a handful of blogs that deal with HIPAA issues. One excellent example, "HIPAA Blog,"[11] maintained by Dallas attorney Jeff Drummond, provides excellent and frequently updated commentary and analysis of developments. Also recommended is the health care industry coverage at Foley Hoag's "Security, Privacy and the

HIPPA continued on page 58

HIPPA continued from page 54

Law."[12] Other useful blogs come from your likely partners in compliance work, the IT sector. For example Redspin Security, one of the leading consulting firms in the field, offers up an excellent blog,[13] All of these will likely become frequent stops for the attorney who works frequently with HIPAA.

Endnotes:

1 Pub.L. No. 104-191, 110 Stat. 1936 (1996).
2 *Id*, § 261 (codified as amended at 42 U.S.C. § 1320d-6 (2006 & Supp. III 2009)).
3 45 C.F.R. §§ 164.302–164.318, plus Appendix (2010).
4 45 C.F.R. §§ 164.500–164.534 (2010).
5 American Recovery and Reinvestment Act, of 2009, Pub. L. No. 111-5, § 13401, 123 Stat. 115, 260 (codified at 42 U.S.C. § 17931(a)).
6 See, e.g. 74 Fed. Reg. 19006 (2009).
7 Va. Code Ann. § 32.1-127.1:03 (2011).
8 *Fairfax Hospitals v. Curtis*, 254 Va. 437, 492 S.E.2d 642 (1997).
9 http://www.hhs.gov/ocr/privacy/index.html.
10 Lena H. Sun, "Clinic Penalized for Not Providing Records," Wash. Post, Feb. 23, 2011, at B04.
11 http://hipaablog.blogspot.com.
12 http://www.securityprivacyandthelaw.com.
13 http://www.redspin.com/blog.

Paul Birch is the Computer Services Librarian at the University of Richmond Law School Library and he teaches legal research in the first year Lawyering Skills program. Paul earned his B.S., M.A. and J.D. from the University of Wisconsin-Madison.