The Health Care Privacy Debate Heats Up*

by Kirk J. Nahra†

September 2007

While Congress and many others continue to discuss whether the current enforcement approach to health care privacy is appropriate, a broader debate is emerging about the suitability of the existing privacy rules in today's evolving health care information environment. Several key recent developments make this debate more interesting and more active—leading to the realistic possibility that new privacy rules for the health care industry (and for many others who use health care information) will be imposed in the near future. Key questions will be whether any new rules target unregulated participants in emerging health information exchange systems or whether changes will seek to further regulate the entire health care industry.

Electronic Health Information Exchanges Drive the Debate

Much of the current debate is being driven by the development of local, state, regional and perhaps national health information exchanges. The Bush administration's push to develop a fully interoperable health information exchange by the year 2014 is focusing attention on whether this new integrated environment requires a new set of health care privacy rules—at least for this setting. While many groups and entities are examining the privacy and security issues presented by health information exchanges, two groups stand out—each having issued important recommendations.

The AHIC Confidentiality, Privacy and Security Workgroup

The Confidentiality, Privacy and Security Workgroup of the American Health Information Community (AHIC) is one of the potentially influential groups dealing with health information exchange privacy and security issues. AHIC is a federal advisory body chartered in 2005 to make recommendations to the Secretary of Health and Human Services on how to accelerate the development and adoption of health information technology. The workgroup was formed in May 2006; its members include representatives of both public and private entities. I chair this

---

* Reprinted from the September 2007 issue of *Privacy In Focus*®.

† Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling for companies facing compliance obligations in these areas. He is the Chair of the firm's Privacy Practice. He serves on the Board of Directors of the International Association of Privacy Professionals, and edits IAPP's monthly newsletter, *Privacy Officers Advisor*. He is a Certified Information Privacy Professional. He can be reached at 202.719.7335 or knahra@wileyrein.com.

workgroup. We are tasked with making recommendations for privacy and security rules in this integrated environment. Recently, the CPS Workgroup issued two key recommendations that relate to how these rules should move forward.

The first recommendation, adopted by AHIC in its June 12, 2007 meeting, provides that:

> *All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements.*

This recommendation focuses on one of the key differences between this health information exchange environment and the original HIPAA environment, a recognition that significant participants in health information exchanges are not covered, either not at all or not appropriately, by the current HIPAA rules. Primarily, this recommendation would have an impact on:

- Health care providers who are not covered entities because they do not bill electronically for their services;
- Personal health records providers who provide services directly to patients, and therefore typically are not covered by the HIPAA rules at all; and
- Regional Health Information Organizations (RHIOs) and other "networks" that play a central role in these efforts, and typically are, at most, considered "business associates" under the HIPAA rules.

Our workgroup was concerned that these players are central to the operation of health information exchanges, and are important elements of emerging health information technologies, but, due to the odd quirks in how the HIPAA rules were adopted (focusing on health care portability and electronic transactions), are not subject to the existing privacy and security rules. This recommendation is designed to bring within the regulated community such participants in the exchange of health care information.

Our second recent recommendation was designed to create a "level playing field" for all participants in these exchanges. The recommendation is as follows:

> *Furthermore, any person or entity that functions as a Business Associate (as described in 45 CFR §160.103) and participates directly in, or comprises, an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements, independent of those established by contractual arrangements (such as a Business Associate Agreement as provided for in HIPAA).*

This recommendation would convert all of these participants into directly regulated "covered entities." Our workgroup believed that different enforcement standards (e.g., potential civil and criminal fines vs. breach of contract) were not appropriate, and that all participants in these

exchanges should face the same rules and enforcement possibilities. This suggestion is clearly not an attack on the HIPAA requirements themselves (although some workgroup members believe HIPAA doesn't work appropriately). Instead, this recommendation recognizes that neither "industry standards" nor "best practices" nor voluntary compliance are sufficient. This is not a recommendation to turn all HIPAA business associates into covered entities—our recommendation relates only to entities that participate directly in health information exchange networks, and would not affect the multitudes of entities that provide services to health care companies without participating in these networks.

This approved CPS Workgroup recommendation also is only a first step—next we will be tackling two additional issues. First, we will be looking at what constitutes a "relevant" HIPAA requirement for particular "direct participants" in a health information exchange network. Clearly, some persons or entities may have an appropriate reason for not needing to meet a particular requirement. The most obvious example involves the information exchange networks themselves, which typically have no relationship with an individual patient and therefore (such as health care clearinghouses under the current HIPAA rules) have little reason to provide a privacy notice directly to individuals.

Second, we will be looking at what, if any, additional confidentiality, privacy or security protections may be needed beyond those already contained in the HIPAA Privacy and Security Rules. Simply translated, our question will be, "Is the HIPAA standard 'good enough' in this context?" We will be focusing our attention on whether today's environment for these information exchanges is materially different from the "HIPAA environment" (recognizing the difficulties posed by determining exactly what the HIPAA environment is) to justify new rules for these health information exchanges.

National Committee on Vital Health Statistics

Following closely on the heels of the CPS Workgroup recommendations, the National Committee on Vital and Health Statistics issued its own set of recommendations, on a generally similar topic. The NCVHS recommendations focused on both the HIPAA standards and the scope of coverage under the HIPAA rules.

NCVHS raised "a significant concern . . . that many of the new entities essential to the operation of the Nationwide Health Information Network (NHIN) fall outside HIPAA's statutory definition of 'covered entity.'" These include a wide variety of entities that may or may not be business associates (along with a wide range of non-covered health care providers). NCVHS concluded that "business associate arrangements are not sufficiently robust to protect the privacy and security of all individually identifiable health information." Accordingly, the NCVHS made the following recommendation (which is entirely consistent with the CPS Workgroup recommendation):

> *HHS and the Congress should move expeditiously to establish laws and regulations that will ensure that all entities that create, compile, store, transmit or use personally identifiable health information are covered by a federal privacy law. This is necessary to assure the public that the NHIN, and all of its components, are deserving of their trust.*

Accordingly, the workgroup and NCVHS recommendations, taken together, raise the need for the integrated health information exchange community to develop new privacy and security laws that ensure that the full range of entities participating in these networks all face the same rules concerning their use and disclosure of health information. These recommendations recognize certain changes in the health care landscape arising from these integrated networks, and the necessity of ensuring that health care information is protected by a uniform standard, without some of the artificial lines drawn by the current HIPAA rules.

Potential New Legislation

The next key development, however, takes the concepts embodied in these recommendations to a far broader level. Specifically, Senators Kennedy (D-MA) and Leahy (D-VT) have introduced new legislation (S. 1814) designed to revamp, almost from scratch, the entire landscape of health care privacy laws. The bill responds to the premise that "fear of a loss of privacy cannot be allowed to deter Americans from seeking medical treatment." Without any particular focus on health information exchanges, this proposal virtually tosses out the HIPAA rules, in favor of a far more restrictive regulatory structure with significantly enhanced risks and penalties for health care companies.
Among the most substantial components of the Kennedy-Leahy bill are:

- Elimination of the Office of Civil Rights as an enforcement agency, in favor of a new Office of Health Information Privacy;
- Creation of an extensive new notice requirement, including a new variety of "opt-out" rights;
- Requirement that companies publicly identify their agents and subcontractors;
- Creation of new "informed consent" procedures, even for treatment and payment uses and disclosures;
- Requirement for authorizations for a wide variety of other disclosures (where none is required today), particularly health care operations;
- Expansion of civil and criminal penalties;
- Authorization for enforcement by State attorneys general; and
- Creation of a private right of action for individuals.

This legislative proposal faces a significant uphill battle. While questions persist about the current enforcement approach to the health care privacy rules, no actual events have indicated a need for new regulatory requirements governing the wide range of practices covered by health care privacy rules today. In fact, particularly in the private sector, the health care privacy rules seem to be working remarkably well. While security breaches are a daily occurrence in many industries, the health care industry has faced only modest problems, almost all of them related to "security" rather than privacy, and most on a relatively small scale (other than the prominent breach concerning the federal Department of Veterans Affairs). Accordingly, the new proposed legislation presents the certainty of disrupting existing operations and creating enormous new costs for the health care industry, without any demonstrated problem that justifies forcing such change.

Conclusion

The renewed debate over health care privacy is just beginning. Clearly, a consensus is emerging that some new rules for the health information exchange environment are needed, mainly to ensure that all participants are subject to a consistent set of legal requirements. There is no consensus on whether these new rules should be tougher than HIPAA; moreover, no consensus whatsoever exists that the HIPAA rules are not "good enough" for the rest of the health care industry. No set of facts to date clearly demonstrates that companies currently covered by HIPAA are ignoring their responsibilities or that personal privacy in the health care environment is not appropriately protected. Accordingly, while the Kennedy-Leahy bill clearly signals the start of an important debate, it seems to be a significant overreaction that would create disruption and expense, without any clearly demonstrated need.

* * *