BNA, INC.

HEALTH IT LAW & INDUSTRY

BNA Employee-Owned Since 1947

REPORT

Reproduced with permission from Health IT Law & Industry Report, 3 HITR 27, 07/04/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

The HIPAA Accounting NPRM and the Future of Health Care Privacy

By Kirk J. Nahra

Mr. Nahra is a partner with Wiley Rein LLP in Washington where he specializes in issues involving health care, privacy, information security and overall compliance litigation and counseling. He is chair of the firm's Privacy Practice and co-chair of its Health Care Practice. He assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. A member of the Board of Directors of the International Association of Privacy Professionals, he is the editor of Privacy Advisor, the monthly newsletter of the IAPP. He can be reached at 202-719-7335 or knahra@wileyrein.com.

I. INTRODUCTION AND SUMMARY

It is fair to conclude that few people would have expected the Health Insurance Portability and Accountability Act accounting rule to create one of the most significant debates about health care privacy in the HIPAA era. Yet, with the release of the Notice of Proposed Rulemaking (76 Fed. Reg. 31426, 5/31/11) to revise the HIPAA accounting right, the Department of Health and Human Services—whether it has meant to or not—has turned the accounting rule into the newest lightning rod for the debate over the future of health care privacy, including the related questions of whether undefined privacy rights will have an impact on the success of various health care reform programs. While there certainly is room for debate on whether the NPRM reflects a sea change in HHS' attitude about health care privacy or simply demonstrates core misunderstandings about the burdens imposed by this NPRM, it is fair to say that the accounting NPRM could create

COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 2151-2876

enormous challenges for the health care industry that could threaten the usefulness of electronic health records and create significant additional expense for the already over-burdened health care industry.

Rather than simply modifying the accounting rule as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, this proposed rule creates a substantial new right for individuals to receive an access report identifying all individuals who have accessed, used or disclosed their information, essentially for any purpose. The justification for this proposed rule is a misguided interpretation of the HIPAA Security Rule that essentially presumes that (a) the Security Rule already requires that every access, use or disclosure of information be tracked and (b) that converting this ''audit log'' information into a patient-specific access report is essentially a simple and automated clerical task. Based on this justification, the NPRM creates this new patient right, without identifying any particular or substantial patient interest that is driving the need for the right. At best, the NPRM explains this collection of data about all uses of information because of the possibility that some individuals would want to determine if there were specific improper uses of their information.

The discussion below highlights the history of the accounting rule, describes the proposed changes incorporated into the NPRM and identifies both significant problems with this proposed rule and additional (and broader) concerns if the intent of this proposed rule is to dramatically alter the balance between patient privacy interests and specific substantial burdens being imposed on the health care industry and its business partners. My conclusion is that this NPRM is fundamentally misguided and should be withdrawn—it relies on an unreasonable interpretation of the HIPAA Security Rule, fails to reflect the technological reality of today's health care environment and mistakenly presumes (even if its assumptions were correct) that creation of this access report will impose little burden, all to support (in a surprisingly untargeted way) an ill-defined and relatively unjustifiable patient interest in learning specific details about the internal activities of health care companies.

II. BACKGROUND

A. The Accounting Rule

The current HIPAA accounting rule was one of the primary ''individual rights'' created by the Department of Health and Human Services in the HIPAA Privacy Rule. While it is fair to say that none of the primary rights (accounting, access and amendment) has been used in high volumes, the accounting rule has been used very infrequently. Many covered entities have received no accounting requests; few have received more than a handful of accounting requests.

The accounting right provides individuals with certain information about specific disclosures of their protected health information. HHS, in the original rule, chose to define the right in terms of disclosures that did not need to be included on an accounting, rather than those that needed to be. The most significant exception to the accounting requirement was the clear and unambiguous exemption for all disclosures for treatment, payment and health care operations, as those terms are defined in the HIPAA rules.

As initial compliance efforts were undertaken, covered entities in many situations built elaborate systems to track data that would be required in the event of an accounting request (including a wide range of approaches to gather information from business associates). Over time, as it quickly became clear that few individuals were going to use this right, companies moved toward a more ad hoc means of responding to accounting requests (to the extent any were received) because it was relatively easy to back into preparing an accounting because of the limited nature of the disclosures that were covered by the rule.

B. The HITECH Changes

Enter the HITECH legislation. The schizophrenic nature of the HITECH law has been well documented. Simply put, Congress desired to incentivize—meaning pay—health care providers to implement electronic health record systems. With arguably typical Congressional logic, because of these incentives—designed to encourage and facilitate use of electronic health records—Congress decided that (1) it would impose new privacy compliance obligations on those who chose to use electronic health records and (2) then would create a new set of privacy obligations for everyone else, unconnected in any way to the use of these electronic health records.

For the accounting rule, HITECH imposed new changes, specific to (although quite imprecisely to) users of electronic health records. The HITECH language provided that this accounting rule exception for *disclosures* of HIPAA protected health information would no longer apply to disclosures ''through'' an ''electronic health record.'' There was a specific compliance time period, based on when a covered entity acquired its electronic health record system.

At the time, most commentators focused on specific issues relating to this language:

- The legislation used the phrase ''electronic health record'' rather than focusing on the ''certified'' electronic health records that were the focus of the incentive payments and the related ''meaningful use'' regulations;
- It therefore was confusing and ambiguous what records were covered (including whether this reference would include health insurers at all or more than a small number of business associates);
- The presumption of Congress seemed to be that the certified records would be able to track these disclosures automatically (although no one believed this presumption to be true); and
- No one really understand what it meant to have a disclosure ''through'' an electronic health record.

These same commentators (myself included) expected that any implementing regulation would restrict application to the certified electronic health records and would target only those health care providers who used the specific records, on the time frame where the relevant technology incorporated this kind of tracking capability.

C. The NPRM

Boy, were we wrong.

Rather than limit the scope of the HITECH provision, HHS clearly and explicitly went far beyond the HITECH statutory language, turning the limited accounting rule into a (somewhat) narrower accounting provision but

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. HITR ISSN 2151-2876

then creating an entirely new access report right that permits individuals to learn about every individual who touches or accesses their protected health information.

So, what exactly did they do? There are lots of important details, but here are the primary highlights.

■ The Accounting Provisions

For the accounting rule itself, HHS is proposing limited changes, designed to limit the burden imposed by the accounting rule and to target the rule to specific patient interests. These changes (*e.g.*, limiting the accounting right to three years, excluding research disclosures and certain health care oversight disclosures) are limited, but generally are useful and well tailored. They create some administrative benefits for a right that today requires little use of resources because it is not used by individuals.

■ The Access Report

The approach to the access report is entirely different. HHS acknowledges that the electronic health records that were the focus of the HITECH legislation do not yet have the technological capability to track this information. Yet, HHS proposes, under its ''general HIPAA authority,'' to create the right to a new access report based on the presumption that the current Security Rule requires tracking of this information across all electronic systems. The problems with this Security Rule interpretation are discussed below. Even if these presumptions were accurate, HHS then proceeds to simply assume that an effective tracking system could, easily and essentially at the push of a button, be turned into an access report.

The intent of this access report ''is to allow individuals to learn if specific persons have accessed their electronic designated record set information'' (76 Fed. Reg. 31429). This ''process of creating'' an access report ''will be a more automated process that provides valuable information to individuals with less burden [than the accounting right] to covered entities and business associates.'' HHS' goal with this proposal ''attempts to shift the accounting provision from a manual process that generates limited information to a more automated process that produces more comprehensive information (since it includes all access to electronic designated record set information, whether such access qualifies as a use or disclosure)'' (76 Fed. Reg. 31429).

HHS provides additional rationale for this new right. HHS believes ''that individuals are interested in learning who has accessed their information without regard to whether the access is internal (a use) or by a person outside the covered entity and its business associates (a disclosure). We believe that the inclusion of both uses and disclosures in the access report significantly increases the benefits to individuals by providing a more complete picture of who has accessed their information'' (76 Fed. Reg. 31436). HHS then makes conclusions about this requirement—and concludes that this is helpful to covered entities and business associates:

> We do not believe that the inclusion of ''uses'' of designated record set information in the access report represents an unreasonable burden on covered entities and business associates. . . . the inclusion of all access, rather than only access that represents a disclosure, may actually be less burdensome on covered entities and business associates than the alternative of configuring systems to distinguish between uses and disclosures of information (76 Fed. Reg. 31436).

This new access report applies to all electronic protected health information in a designated record set (rather than just the ''electronic health record'' identified in the HITECH law) ''because we believe that this greatly improves transparency and better facilitates compliance and enforcement, while placing a reasonable burden on covered entities and business associates'' (76 Fed. Reg. 31437).

■ The HIPAA Security Rule

This idea of ''burdens'' imposed on covered entities and business associates is a core element of the NPRM. Essentially, HHS believes that (1) the HIPAA Security Rule already requires that all of the ''access report'' information already must be tracked to be in compliance with the Security Rule (and even must be part of the current ''reasonable and appropriate safeguards'' that are applicable to business associates); and, therefore, (2) creating the access report will not be a significant burden. While the access report promises to create significant burdens for virtually any covered entity—whether or not individuals begin exercising this newly created right—the most significant impact of this NPRM may in fact be on a topic that isn't even part of the NPRM, as through the back door, HHS has fundamentally revised its overall approach to the HIPAA Security Rule.

From the beginning, HHS developed a ''flexible'' approach to compliance with the Security Rule, by (1) making the requirements ''scalable'' based on the specific operations and activities of the organization; (2) developing a rule that was ''technology neutral''—meaning that the Rule does not dictate any specific technological solution; and, as clearly described in the Rule under the heading of ''flexibility of approach,'' (3) making clear that ''Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.'' (45 C.F.R. § 164.306(b)).

The overall approach was summarized by HHS in one of its own educational papers on the HHS Security Rule.

> The Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The Rule allows a covered entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications. A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.

See HIPAA Security Series, #4 ''Security Standards: Technological Safeguards,'' available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.

In this same paper, HHS further states:

> The Security Rule does not require specific technology solutions. In this paper, some security measures and technical solutions are provided as examples to illustrate the standards and imple-

> mentation specifications. These are only examples. There are many technical security tools, products, and solutions that a covered entity may select. Determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for their specific organization, given their own unique characteristics, as specified in § 164.306(b) the Security Standards: General Rules, Flexibility of Approach. *Id*.

In the NPRM, however, it seems to have fundamentally rejected this approach. The discussion of this issue in the NPRM focuses on two components of the Security Rule. One applicable provision falls under the ''technical safeguards'' component of the Rule. Pursuant to this provision, as a ''Standard,'' a Covered Entity must have ''audit controls,'' meaning to ''[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.'' 45 C.F.R. § 164.312(b). There is also a separate implementation specification, as part of the ''Administrative Safeguards'' in the Security Rule, for ''Information system activity review,'' which requires a covered entity to ''[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.'' See 45 C.F.R. § 164.308(a)1(ii)(D).

In the NPRM, HHS asserts that ''[b]y limiting the access report to electronic access, the report will include information that a covered entity is already required to collect under the Security Rule''—simply because of the Security Rule provision that requires a covered entity ''to record and examine activity in information systems and to regularly review records of such activity'' (76 Fed. Reg. 31429). Based on this regulatory provision,

> We believe that this is reasonable since all such covered entities and business associates are required by the Security Rule to maintain access logs and, therefore, should be able to provide this information to individuals in response to requests. We believe that the administrative burden on covered entities who are complying with the HIPAA Security Rule will be reasonable, in light of their existing obligation to log access to electronic protected health information (76 Fed. Reg. 31427).

Based on these two provisions (and there is precious additional detail in any applicable discussion of the Security Rule), HHS has presumed that (1) there is only one way to meet these specific provisions of the Security Rule and (2) that if you are doing that—and you MUST be doing this—compliance with the access report obligation will essentially be automatic and easy.

III. OVERALL IMPLICATIONS

There is an enormous variety of concerns about this proposal. Many of the issues are ''detail'' points that, collectively, are quite significant. HHS has made numerous presumptions about the state of the industry, distorted the results of its own request for information that preceded this NPRM, casually made conclusions about other portions of the HIPAA rules and made numerous broad and sweeping generalizations. Each of these issues will need to be addressed at some point. Here, however, I focus on the ''big picture'' concerns about this proposed regulation, and highlight some of the broader concerns and issues raised by this proposal.

A. What is the patient privacy interest being addressed?

It is somewhat hard to understand exactly what individual privacy interest is being served here. HHS acknowledges that few individuals have exercised their accounting right. It is also fair to say that this *may* be because the right is so limited (but that conclusion also presumes that individuals are sophisticated enough to recognize that this right exists but then can conclude that it was limited in its reach).

The primary ''interests'' identified in the NPRM seem to revolve around learning whether inappropriate individuals have accessed PHI. If that is the interest to be served, why require a report that tracks the enormous volumes of individuals who access information for appropriate and legitimate reasons, virtually all of whom would be unknown to the individual? Hardly a ''minimum necessary'' approach to serving this interest.

On a broader level, if some patients want to learn each individual who accessed their information, even if each one is acting appropriately to perform specific job functions, why is that an interest that we should accommodate? Is this some inherent privacy interest? What is the rationale for creating this new right? HHS presents no explanation of where this ''right'' comes from or why—particularly given the history of both the accounting rule and the other individual rights—HHS is creating this new compliance obligation.

B. Are there other interests at stake not considered by the NPRM?

And, if individuals really start asking for these access reports, isn't that going to create more problems? What can we expect individuals to do with a list of every person who accessed their information—a laundry list of people who they typically will know nothing about.

Primarily, isn't there a risk to these employees and others whose identities are being disclosed to individuals? HHS recognizes that these reports should not include the identities of other patients who might have accessed information (for example, a patient who receives someone else's claim information). However, there is no acknowledgment at all about the potential risks to employees, even if this is not classified as an employee privacy right. Presumably, some (and maybe many) of the individuals seeking this access report will have some gripe—one that could be aggressive or threatening. Aren't we putting employees at risk by identifying them to patients?

Moreover, isn't there a significant risk that these access reports will be misused for purposes having nothing to do with privacy? It is not hard to imagine use of this list in a malpractice suit, for example, to demonstrate that someone did or didn't review a record, or didn't look at it enough or at the right time. Is there enough justification for this privacy interest—whatever it is—to offset these negatives (even before getting to the burden and cost implications)?

C. Is this a reasonable way to look at the security rule?

Perhaps the most significant impact of the accounting rule NPRM is the through-the-back-door reinterpretation of the HIPAA Security Rule. Even if the

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. HITR ISSN 2151-2876

accounting rule/access report proposal is scrapped, covered entities and business associates still need to be aware of this new interpretation of the Security Rule.

As discussed above, HHS' view of the Security Rule requirements seem to be fundamentally at odds with its approach since the rule was published in 2003. This new interpretation—unlike everything else they have said—is that there is no flexibility, no scalability, no ability to determine appropriate security procedures based on a company's risk assessment. Instead, you must track everything, and must have it in a way that matches this new access report, period.

Specifically, this approach is different from HHS *own* (limited) guidance on these specific issues. In its preamble and commentary to the Security Rule, for example, in responding to a comment about the appropriate heading for this requirement, HHS stated that the meaning of the requirement ''is to have the capability to record and examine system activity. We believe that it is appropriate to specify audit controls as a type of technical safeguard'' (68 Fed. Reg. 8355). HHS also stressed that ''[e]ntities *have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses*.'' (emphasis added) (68 Fed. Reg. 8355). HHS also stated that ''[w]e support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity's care'' (68 Fed. Reg. 8355).

Moreover, even on the particular provisions at issue, HHS has made clear that there is no one specific ''answer'' to the security rule obligation. In its discussion of the ''audit control'' standard, HHS states:

> Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred. It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use EPHI.

See HIPAA Security Series, #4 ''Security Standards: Technological Safeguards.''

Further, for the ''information system activity review'' requirement (as described in the HIPAA Security Series, #2 ''Security Standards: Administrative Safeguards,'' available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf), HHS states only that:

> Information system activity review procedures may be different for each covered entity. The procedure should be customized to meet the covered entity's risk management strategy and take into account the capabilities of all information systems with EPHI. Id. at 6.

Accordingly, it is extraordinarily difficult to reconcile everything HHS has said about the Security Rule to this point with this new interpretation from the NPRM—which is set forth essentially as an assumption without any acknowledgment of a complete change in interpretation.

D. How much burden is a tolerable one?

Even aside from this core change in Security Rule approach, HHS makes one additional (and quite enormous) leap: because (it asserts) companies are required to track access to information, therefore it is easy to prepare an access report that tracks all such access to and uses and disclosures of information, across all electronic systems for covered entities and business associates. Again, this assertion is made without any specific evidence, basically as a matter-of-fact presumption.

At its core, this assumption seems to fly in the face of the purpose of these requirements. The purpose is to allow covered entities to monitor access to information. Even if done consistent with the Security Rule interpretation, it tracks this information by employee (or system user), rather than by patient. This information is meant to be reviewed—and therefore can be checked if the need arises in particular places for particular reasons. Yet, HHS simply assumes that (1) it is easy to compile all of this information across a company's various systems (combined with an erroneous assumption that there is a single ''designated record set system); (2) that it is also easy to pull and compile this information across all business associates; and (3) that this information can be reviewed by individual patient record, rather than by employees. Why is it reasonable to presume that a system designed to track employee behavior would automatically also permit tracking by patient?

Accordingly, this NPRM creates real questions about the basis for these new burdens, which HHS minimizes by assuming the burdens away.

E. Are we changing the privacy balance?

The accounting rule NPRM—if adopted in its current form—will create substantial burdens and costs for health care entities and their business associates, with little clear benefit to most individuals and new risks for employees and others based on these new access reports. With that said, the larger impact of this NPRM *may* be that HHS is fundamentally re-evaluating its overall approach to patient privacy. Does this NPRM presage a new focus on transparency and patient control, essentially independent of the burden imposed on industry? Are the HIPAA rules (and related implications in other areas) being reconsidered so that the current regulatory structure is at risk?

There is no basis to conclude with any certainty that this NPRM reflects anything more than a mis-guided balancing of interests based on a misunderstanding of these interests and the practical impact of the proposal. It is quite possible that a final rule will reflect either a fundamental reconsideration of the entire NPRM approach or a dramatically altered proposal that reduces the burdens and impact of this proposal dramatically.

But this may not be true. We may be seeing continued steps to break-up the current structure. There clearly are steps being considered in this regard—the ''opt-out'' proposal as part of the proposed Accountable Care Organization regulation and the continuing interest in a health information exchange structure that imposes new and broader patient consent requirements,

even at the risk of threatening the benefits that are possible with these HIEs.

Here, we have HHS expanding an existing right that few people have been using, because of what seems to be the possibility that a small number of people will want to know something about who accessed their information (because there is the possibility of inappropriate access, there is simply curiosity or there is a value in the ''transparency'' of health care company operations). HHS seems to agree that this interest—whatever it is—will be used by a limited number of individuals, and will generally not apply to most of what is covered by the access report (*e.g.*, individuals will want to ask about specific people accessing their information, while the ''right'' could apply to everyone who touched the information). Yet, it is willing to create this substantial burden, simply on the assumption that these capabilities already exist and are being used, even though it clearly concedes that this is not true for the core electronic health records that started this analysis under HITECH in the first place.

IV. CONCLUSION

The HIPAA accounting rule NPRM is fundamentally misguided. It expands existing rights without any demonstrated need or clear benefits. To the extent a demonstrable privacy interest exists, this obligation is not remotely tailored to achieving this interest. Therefore, there is little ''privacy upside'' from the creation of this new right.

At the same time, HHS has missed badly on its view of the compliance burden. It has re-interpreted the HIPAA Security Rule – through a casual and passive presumption – in ways that are unreasonable and inconsistent with its prior approach. It also has fundamentally erred in its understanding of the burdens that will be imposed on the health care system through this NPRM. There are ways of reducing this burden—for example, through minimizing the scope of information that is covered by this NPRM (through clarification of whether HHS wants this only to apply to a single designated record set, rather than any information that is a part of a designated record set, wherever that information may be). However, at its core, HHS should withdraw this proposal for the creation of a HIPAA right to an access report, and should go back to the drawing board in implementing the HITECH accounting requirement. The current proposal will provide little benefit to patients, and these benefits could be achieved through much narrower means. Moreover, in reaching a balance, HHS has missed badly in weighing the costs and burdens on health care companies from these proposed obligations.

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. HITR ISSN 2151-2876