NACDS NATIONAL ASSOCIATION OF CHAIN DRUG STORES

VIA: http://www.regulations.gov

ATTENTION: HIPAA Privacy Rule Accounting of Disclosures

August 1, 2011

The Honorable Katherine Sebelius
Secretary, U.S. Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue, S.W.
Hubert H. Humphrey Building, Room 509F
Washington, DC 20201

Dear Madam Secretary:

Re: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act; Notice of Proposed Rulemaking – RIN 0991-AB62

413 North Lee Street
P.O. Box 1417-D49
Alexandria, Virginia
22313-1480

The National Association of Chain Drug Stores (NACDS) appreciates the opportunity to comment on proposed regulations of the Department of Health and Human Services Office for Civil Rights (HHS) with respect to the expansion of the accounting of disclosures requirement under the Health Information Technology for Economic and Clinical Health ("HITECH") Act.

The National Association of Chain Drug Stores (NACDS) represents traditional drug stores, supermarkets, and mass merchants with pharmacies – from regional chains with four stores to national companies. Chains operate 39,000 pharmacies, and employ more than 2.7 million employees, including 118,000 full-time pharmacists. They fill nearly 2.6 billion prescriptions annually, which is more than 72 percent of annual prescriptions in the United States. The total economic impact of all retail stores with pharmacies transcends their $830 billion in annual sales. Every $1 spent in these stores creates a ripple effect of $1.96 in other industries, for a total economic impact of $1.57 trillion, equal to 11 percent of GDP. NACDS represents 137 chains that operate these pharmacies in neighborhoods across America, and NACDS members also include more than 900 pharmacy and consumer packaged goods suppliers and service providers, and over 60 international members from 23 countries. For more information about NACDS, visit www.NACDS.org.

Introduction

We appreciate that HHS has actively engaged with covered entities in the various rulemakings to implement the privacy provisions under the HITECH Act. We also appreciate that HHS has sought to balance the needs of individuals with the burden on the health care delivery system. We have applauded a number of HHS' previous proposals.

(703) 549-3001
Fax (703) 836-4869
www.nacds.org

However, we believe that this proposed rule, in particular with respect to the new "access report," fails to adequately and accurately apply the requirements of the HIPAA Security Rule and take into account the technological capabilities of the retail pharmacy industry. Accordingly, we urge HHS to withdraw the proposed access report requirement. We suggest HHS use the Request for Information (RFI) process to narrowly tailor the specific questions it seeks to address and allow covered entities to comment on existing practices and what could be possible in the future within reasonable timeframes.

Scope of NPRM

In the applicable HITECH Act provisions, Congress clearly stated that for the revisions to the accounting rule, HHS was to "only require such information be collected through an electronic health record in a manner that takes into account the interests of the individuals interested in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures." We believe that HHS has given undue deference to issues that *might be of interest* to individuals, without appropriately considering or weighing the disproportionate burden on covered entities. Moreover, HHS is basing its decision to require the access report on incorrect assumptions and faulty conclusions.

As we commented to HHS in 2010 in response to HHS' RFI on these matters, as HHS considers the expansion of the accounting of disclosures requirement, HHS must first consider the scope of this expansion. In particular, just because health information is stored in or disclosed through a computer does not equate that computer system to an electronic health record. We feel compelled to restate the concerns we had raised in 2010 in response to the RFI, provided below.

As HHS had properly recognized in the Federal Register notice for the RFI, and as we mentioned above, under the HITECH Act the exemption from the accounting of disclosures requirement under the HIPAA Privacy Rule for disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures *through an electronic health record*. Section 13400 of the HITECH Act provides an extremely broad definition of "electronic health record." As such, HHS should be guided by Congressional intent when determining what falls under the definition of "electronic health record."

Congressional intent can be determined by reviewing the HITECH Act as a whole. Notably, the HITECH Act provides grant funding for certain providers to adopt electronic health records and provides a mechanism for the development of criteria for determining eligibility for such funding. It is logical to conclude that Congress intends for the expanded accounting of disclosures functionality (i.e. removal of exemption) to apply to providers who are eligible to receive funding for, and actually adopt, electronic health records as they are envisioned under the provisions of the HITECH Act. Since not all health care providers are eligible for grant funding for the adoption of electronic

records, it is clear that Congress intended for certain providers to adopt a certain type of electronic health record, and for specific requirements to attach to those electronic health records.

The logic that the expanded accounting of disclosure requirement applies to providers who are eligible to receive funding for, and actually adopt, electronic health records as they are envisioned under the provisions of the HITECH Act is supported by the historical record of the HIPAA Privacy Rule. Specifically, HHS recognized under the original final HIPAA Privacy Rule that "the additional information that would be gained from including these [treatment, payment, and health care operations] disclosures would not outweigh the added burdens on covered entities."[1] Since most covered entities, including pharmacies, are using the same, or substantially similar, computer systems as they did when the original HIPAA Privacy Rule was finalized, HHS would have to reach the same conclusions with regard to burden versus benefit for these computer systems as they did in December 2000.

As HHS is aware, pharmacies are not among the entities that are eligible for grant funding under the HITECH Act for the adoption of electronic health records. Moreover, we refer HHS to a recent letter submitted to Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) regarding existing pharmacy computer systems, which stated the following:

> It is critical to ensure that all health care providers have access to an interoperable exchange of health information through certified EHRs and other HIT systems. Specifically, in pharmacy, computerized records are considered databases that are generally not interoperable in a manner to meet the objectives described for certified EHR technology.[2]

Consequently, we believe that pharmacy computer systems are not "electronic health records" as such term is defined under the HITECH Act.

---

[1] At 65 Fed Reg 250, p. 82739; HHS recognizes the following:
"While including all disclosures within the accounting would provide more information to individuals about to whom their information has been disclosed, we believe that documenting all disclosures made for treatment, payment, and health care operations purposes would be unduly burdensome on entities and would result in accountings so voluminous as to be of questionable value. Individuals who seek treatment and payment expect that their information will be used and disclosed for these purposes. In many cases, under this final rule, the individual will have consented to these uses and disclosures. Thus, the additional information that would be gained from including these disclosures would not outweigh the added burdens on covered entities. We believe that retaining the exclusion of disclosures to carry out treatment, payment, and health care operations makes for a manageable accounting both from the point of view of entities and of individuals."

[2] Letter to Department of Health and Human Services Office of the National Coordinator for Health Information Technology from Academy of Managed Care Pharmacy, American Pharmacists Association, American Society of Consultant Pharmacists, American Society of Health-System Pharmacists, and National Community Pharmacists Association; May 10, 2010; page 3.

If HHS believes that electronic health records will not be capable of meeting the statutory deadlines for complying with the provisions of the HITECH Act, then HHS should use its regulatory authority to address that concern. HHS should not, however, seek to circumvent this difficulty by imposing a requirement for a new access report that has no precedent and does not flow from any existing HIPAA or HITECH provision, rule, or obligation.

Proposed Modifications to Accounting of Disclosures Rule

We generally support HHS' proposed revisions to the existing accounting of disclosures requirement. As HHS recognizes, individuals have demonstrated limited interest in their right to receive an accounting of disclosures. Our smaller members have each received no requests or few requests for an accounting of disclosures since the accounting rule became effective in 2003, while our larger members have received few requests per capita. However, when an individual request is received, a significant investment of time and resource is typically required to respond to the individual's request.

We applaud HHS for proposing the following modifications to better balance the burdens of the accounting requirement with the interests of individuals:

- Reducing the accounting period from six years to three years.
- Establishing an affirmative list of categories for which an accounting is required. However, we request a good faith standard with respect to the exceptions to the list. A covered entity may not be aware that a disclosure had been made for a purpose that was excluded. The covered entity should not be penalized for including in the accounting such disclosure if the covered entity did not, or could not reasonably, know such purpose.
- Excluding from the accounting report disclosures where a breach notification letter was already provided to the individual.
- Limiting accounting of disclosures requirement to the designated record set, so long as HHS clarifies that the accounting report is limited to disclosures of the covered entity's "official" designated record set(s), and not to copies of information or pieces of data that also happen to be included in the designated record set, including copies of information and data held by business associates. We presume that this is HHS' intent, but request that HHS clarify this point. If HHS' intent is to require something broader, then we would urge HHS to reconsider, as any intent broader than our assumption would provide little to no benefit and would only serve to maintain the existing imbalance of the benefit to the individual of the accounting right versus the burden to covered entity to collect and produce the information needed for an individual report.

NACDS Strongly Opposes the New Access Report Proposal

With the access report proposal, we believe that HHS would create a new privacy right based upon a misapplication of the HIPAA Security Rule. Moreover, the proposed rule would create the new access report with little justification, and based on a significant underestimation of the burden to be imposed on covered entities and business associates.

Misapplication of Security Rule

The existing HIPAA Security Rule provides flexibility of approach to allow individual covered entities to decide what methodology best applies to their businesses operations. The current approach allows covered entities to fully consider the scale of their health care operations and the technical solutions that will best achieve compliance.[3] The concept behind the existing rule underscores the fact that what may be feasible for a small covered entity may not be technologically or operationally practicable for a large-scale operation, or vice versa, and that individualized methodologies that achieve the same regulatory intent are the best approach to this rule. The underlying concept was best captured by HHS in one of its own guidance documents on the 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. … The Security Rule does not require specific technology solutions. In this paper, some security measures and technological solutions are provided as examples to illustrate the standards and implementation 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 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.

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

In the NPRM, however, HHS has turned this approach on its ear. HHS' view of the Security Rule requirements in the NPRM contradicts everything it has published about the Security Rule to date. This new interpretation eliminates flexibility, scalability, and ability to determine appropriate security procedures based on a company's risk assessment or cost benefit analysis. Instead, according to the NPRM, covered entities and business associates must track everything in audit logs, and must be able to quickly transform those audit logs into a readily-understandable "access report."

[3] 45 CFR 164.306(b)

As mentioned above and in several publications on this NPRM, the current Security Rule does not require the level of logging anticipated by HHS and deviates from the industry interpretation of the audit logging obligations for covered entities.

> 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. … [I]t relies on a misguided 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.
>
> (*See* Kirk J. Nahra, The HIPAA Accounting NPRM and the Future of Health Care Privacy, 3 Health IT Law & Industry Report 27 (BNA) (2011)).

HHS does not appear to fully understand the actual policy and practice of how covered entities have interpreted and implemented the HIPAA Security Rule. Even assuming this level of data is being captured, many current pharmacy systems record data by user ID, rather than by individual patient. The focus of the HIPAA Security Rule is to set safeguards around the security and access of patient information. With this in mind, health care providers have created systems to monitor and audit individual employee uses (e.g. by user ID), rather than by individual patient. Many industry entities have established cataloging systems that classify the data by the user ID, and HHS' interpretation of the Security Rule will force the entities to re-catalog all of this information or create an application that filters voluminous amounts of data by the patient identification information. Essentially, to be able to generate an access report for a patient, a typical chain pharmacy would have to plan and implement significant programming and redesign of all pharmacy systems that access patient information that could possibly be contained in a designated record set. This will take many millions of dollars and multiple years to accomplish.

Thus, considering the long and well-documented history of HHS' flexible approach to the Security Rule, it is extraordinarily difficult to reconcile this flexible approach with this new interpretation from the NPRM, which is set forth essentially as an assumption without any acknowledgment of a complete change in interpretation. Accordingly, we urge HHS to withdraw this discussion of the Security Rule in the context of its overall re-examination of this entire NPRM.

Role-Based Access

As another example of how many pharmacies have implemented the provisions of the Security Rule, which is likely to be representative of other covered entities, we ask HHS to consider how audit logs and role-based access may be used together to support an appropriate security environment. When roles are defined discretely, each individual employee is allowed access only to the information that he or she needs to perform her or his duties. These role-based limitations greatly diminish the likelihood that any individual employee would inappropriately access PHI that she or he does not need access to perform her or his job. Role-based access eliminates any need for creating or retaining a detailed log of employee 'views' of data; by definition, the pre-determined role limits the employee from viewing more data than is needed to perform his or her job. In these cases, rather than create detailed access logs of all employee 'views' of data, a covered entity might instead make risk-based and cost-benefit-based decisions in keeping with the Security Rule's flexibility of approach, using audit logs to identify, track and investigate any inappropriate ***actions***, such as printing, downloading or modifying. View-only access might be captured in cases where the screen viewed portrays "high risk data" such as diagnosis, Social Security number, or financial account number, as an extra precaution against employees acting with malicious intent. By contrast, indiscriminant logging of employee 'views' of benign data, such as patients who filled a prescription with no reference to the medication prescribed, has no value in an appropriately-crafted security program. To require now that such activity would be logged for privacy concerns eliminates the flexibility of approach built into the Security Rule and adds little to no benefit to the overall security of PHI.

HHS Underestimates Burdens

In light of each covered entity's reliance on HHS' longstanding flexible approach applied to the Security Rule, the proposed access report requirement would now impose enormous new burdens that HHS has not considered in the NPRM. The cost to the pharmacy industry would be staggering and nearly impossible to quantify with any reasonable certainty. For most pharmacies, it would most likely be a multi-million dollar project, as opposed to the $30 per pharmacy that HHS estimates.

The technical burden of creating an access report would be very high. It would require significant complexity that is not in place today. The access report would require many pharmacy computer systems to be completely redesigned and redeployed. This would require years of research, design, development, testing, rollout, and training.

To provide a *limited example* of the increased cost of the proposed new access report, we have calculated the approximate increased data storage cost created by the new access report. For a typical chain pharmacy that could fill well more than 100,000,000 prescriptions annually, the estimated three-year *data storage* cost (for a system that would have to be created from scratch) will exceed $500,000. This number is based on an estimate of the amount of storage space required for one logged entry for one individual system user for one activity (approximately 200 bytes) multiplied by the

volume of prescriptions annually filled by a typical chain pharmacy (more than 100,000,000) and the average number of people included in the filling process (eight). (NOTE: All of these numbers are conservative estimates.) This data storage cost has never been required previously and would result in a substantial financial burden to a covered entity.

A covered entity would also incur an additional financial burden to acquire and maintain access report information from their business associates. The proposed rule requires a covered entity to gather access report information for each business associate, rather than direct a patient to the business associate to obtain the information. To be able to respond to a patient's access report request within the proposed 30-day time limit, it could be necessary to establish regular data transmissions of each business associate's access report information, instead of imposing an even more strict time limitation on the affected business associate(s) to provide the information in less than 30 days, in order for the covered entity to collect, compile, and process the requested report. This would result in substantially more electronic storage space to retain the access report information from each business associate, and an additional substantial cost and financial burden to the covered entity.

Significant Burden, Little Benefit

We have trouble identifying any specific individual privacy interest that would be served by the proposed rule, beyond simple curiosity. We see no reasonable basis from a privacy perspective to mandate that individuals be given such details about the internal operations of every covered entity and business associate.

HHS notes throughout the NPRM that the purpose of this new access report right is to provide greater transparency to the patient into uses of the patient's health care information. "We believe that these two rights [accounting of disclosure and right to an access report], in conjunction, would provide individuals with greater transparency regarding the use and disclosure of their information than under the current rule."[4] However, the proposed rule as currently drafted does the opposite. If implemented as written, the proposed access report will create more unnecessary questions from patients about legitimate uses and disclosure of their health care information during the normal pharmacy filling process.

HHS also notes that typical patients who will be requesting such reports will be more interested in who is accessing their patient information, rather than what information was accessed. We fear that despite the fact that the purpose of this proposed rule is to provide greater transparency into legitimate/illegitimate uses of patient health care information, these reports could be used by individuals who have some sort of problem with one of the employees – one that could be hostile or threatening.

[4] 76 Fed Reg. 31429

For illegitimate employee access to patient information, patients should already receive notification through the HIPAA breach rule or through the current accounting of disclosure requirements. For instance, if an employee inappropriately accessed a patient's information, this access would be evaluated under the HIPAA breach significant risk of harm standard. If the situation created a significant risk of harm to the patient, the covered entity would be required to provide the patient with a breach notification letter. If the incident did not create a significant risk of harm, the covered entity would be required to log an accounting of disclosure which would be made available to the patient upon request. These tools should provide the patient the information needed to determine if someone has accessed his or her information without proper authority.

Instead, we believe this new access report right would create unnecessary confusion, frustration, and anxiety among patients who request this information because of the volume of information that will be included on the report. For example, the average pharmacy prescription is handled by approximately eight different pharmacists and technicians during the filling process, each performing an essential function in connection with the filling and dispensing of the prescription and claims adjudication processes. If a patient received one maintenance medication each month for a year, a report of pharmacist and technician views would result in 96 lines of data. A standard 8.5" x 11" piece of paper holds approximately 60 lines of data. Thus, this report covering the prior three years as required by the rule, would result in an almost five page, single spaced report. The average patient who is 65 years old or older fills about eight prescriptions per year, which would result in a longer report for a patient who most likely will not understand why his/her three-year access report is 38½ pages long, also single spaced. Those estimates account only for pharmacist and technician views, and not for supporting, legitimate job functions that also may access records, such as IT support or mail order fulfillment.

Furthermore, the proposed report would contain only the accessing employee's name, date and time of access, the description of the information accessed, and the description of the activity. These pieces of information may be confusing to the patient, difficult to read and understand, and may cause undue frustration and anxiety as to why so much information is recorded and accessed for one monthly maintenance medication.

We believe that the technological and financial burden to implement the proposed access report right rule far exceeds the benefit to the few patients who will request this type of report each year. Considering the lack of benefit that we can see weighed against the vast burdens to covered entities and business associates, we must urge HHS to reconsider the access report requirement. In the NPRM, HHS recognizes that few individuals will request an access report, which only strengthens our belief that the benefits to individuals are greatly outweighed by the burdens. The fact that few requests will be made does not in any way diminish the technologic and systems burdens that would have to be overcome.

Employee Privacy

As mentioned above, despite the fact that the purpose of this proposed rule is to provide greater transparency to uses of an individual's patient health care information, these reports could be used by individuals who have some sort of problem with one of the employees – one that could be hostile or threatening.

Because of these concerns, if HHS continues to move forward with the proposed access report, we encourage HHS to revise the requirement to include only the employee's position or title on the report. For example, taking this approach would allow an individual to know if a "pharmacist" or "technician" accessed the individual's information without disclosing the employee's name. This modification would work to protect the privacy of the individual employee, while providing the individual with information as to who accessed his/her information.

Cost Concerns

Unfortunately, the substantial costs of complying with the NPRM likely will have to be absorbed into the costs of services provided, resulting in an increased financial burden to the patient in an already stressed economic environment. In many segments of the health care industry, patient costs are covered by commercial or government insurance, where rates are negotiated and set in advance for a fixed period of time. This means that initially, the increased financial burden will likely be borne by those patients paying cash out-of-pocket for their pharmaceuticals. As with many patients in the United States who have limited discretionary income to spend on health care, prescription medications may be filled less often.

Confusion about Affected Information and Compliance Dates

Should HHS decide to move forward with the adoption of an access report requirement, despite our serious concerns, then the access report requirement should only extend to those specific electronic systems that contain the actual designated record sets. Although limiting the approach in this manner would still carry all the concerns we raise in this letter, it would keep the requirement within the realm of the possible. Otherwise the tracking requirement would be limitless. For example, there would be confusion about how far down the chain of business associates the requirement would stretch. Moreover, differing electronic and system standards would exponentially increase the time and resource necessary to fully comply.

The confusion about the affected information arises from the variety of terms that HHS uses in the NPRM. In addition to the term "designated record set," HHS uses the terms "designated record set information" and "designated record set system." When the term "information" is added to the phrase "designated record set," this new term could be interpreted to require an access report from any entity that has any of the information from a designated record set. That would appear to require a covered entity to contact every other entity that has any of that information, without any reasonable restriction on who that would be or what component of the information.

The use of the term "designated record set system" may reflect a fundamental misunderstanding. There is no such thing as a designated record set "system." We suspect that this term may originate from HHS' attempt to reconcile the electronic health record language of the HITECH Act with the access report requirement. This is a reconciliation that cannot occur in this manner. In fact, HHS has recognized elsewhere that designated record sets can be held in multiple systems and by multiple entities. Consequently, there is no rational basis to connect compliance time periods to purchases of a "system," when such "system" cannot really exist. HHS must reconsider how its understanding of this phrase affected its reasoning in the NPRM, as part of its overall consideration of this proposed rule.

HHS' proposed compliance dates are both inappropriately designed, as they are based on a misunderstanding of the systems where a designated record set would exist, and impractical and infeasible for all the reasons set forth above. HHS must significantly extend the compliance dates should it choose to allow any portion of the access report requirement to go forward.

Confusion about the Term "Access"

Again, should HHS decide to move forward with the access report requirement, HHS must provide a definition of the term "access" that should apply to database records that are searched and selected, as opposed to records that are merely searched. In the course of health care delivery, various records must be searched to identify the one that is needed. In response to a search request, an application will return records that meet the selection criteria and the application will provide a list for the user. To log every record returned by a search as having been accessed would require enormous technical modifications as well as enormous amounts of storage space. Such a requirement would make the access report provision so unwieldy as to approach the impossible.

Additional Business Associate Concerns

Finally, under the current HIPAA Security Rules, business associates are obligated to "implement administrative, physical and technical safeguards that reasonably and appropriately protect the electronic protected health information" it receives.[5] The proposed rules issued on July 14, 2010[6] that would require business associates to directly comply with the HIPAA Security Rule are not yet in effect. It is unreasonable to assume that a business associate has already implemented systematic changes required by the HIPAA Security Rule before the business associate is required to by regulation. Consequently, it is unlikely that business associates will have the technical ability to provide access reports to a covered entity when requested by patient, or to have captured data for the previous three years. Therefore, if HHS should move forward with an access report requirement, HHS should mirror the requirement in the accounting of disclosures

[5] 45 CFR § 164.314(a)(2)(i)(A)
[6] 75 Fed. Reg. 40868.

rule and allow a covered entity to provide the patient with a list of business associates and contact information to allow the patient to contact the individual business associates for information that would be included in the access report.

Conclusion

We thank HHS for the opportunity to comment on this NPRM, and urge HHS to reconsider the access report requirement. With this proposal, we believe that HHS has failed to appropriately balance the benefits to patients against the burden to covered entities. HHS has improperly applied the HIPAA Security Rule and failed to consider the costs and consequences of the proposed access report requirement. This regulation would require dramatic and expensive new systems, with enormous financial, technical, and administrative resources, for a very limited and questionable patient interest. We urge HHS to review its mandate under the HITECH Act and begin anew in a manner that we have recommended herein.

Sincerely,

/s/

Kevin N. Nicholson, R.Ph., Esq.
Vice President
Government Affairs and Public Policy