VIA http://www.regulations.gov

May 21, 2009

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building
Room 509F
200 Independence Ave, SW
Washington, DC 20201

Re: HITECH Breach Notification

Dear Sir/Madam:

Surescripts, LLC appreciates the opportunity to provide comments to the Department of Health and Human Services ("HHS") regarding its guidance for technologies and methodologies that render protected health information ("PHI") unusable, unreadable, or indecipherable to unauthorized individuals under the Health Information Technology for Economic and Clinical Health (HITECH) Act ("Act"), and the breach notification provisions of the HITECH Act. We hope that our perspectives are helpful to HHS as you draft rules to implement the breach notification provisions and consider updates to the guidance.

BACKGROUND

As a matter of background, Surescripts is the result of the merger in June 2008 of SureScripts, LLC and Rx-Hub, LLC. SureScripts, LLC was founded in August of 2001 by the National Association of Chain Drug Stores (NACDS) and the National Community Pharmacists Association (NCPA), which together represent the interests of the 55,000 chain and independent community pharmacies throughout the United States. RxHub, LLC was founded in the same year by the nation's three largest pharmacy benefit managers (PBMs) – CVS Caremark Corporation, Express Scripts, Inc. and Medco Health Solutions, Inc. RxHub's expertise in patient identification and delivering drug benefit information to the physician at the point of care complements SureScripts' focus on electronic prescription routing from the physician's office to the pharmacy. The merger combines these strengths with a shared focus on more access to patient medication history to form a single suite of comprehensive e-prescribing services.

The new organization enables physicians to securely access vital health information when caring for their patients through a fast and efficient health information exchange. This will allow them to transmit electronic prescriptions and renewal requests to both community and mail-order pharmacies. In 2008, the combined organization routed 68 million electronic prescriptions, responded to more than 78 million requests by physicians confirming information about their patients' prescription benefit and delivered 16 million prescription histories. With appropriate patient consent, the combined organization will extend this information to clinicians caring for more than 65 percent of patients across the United States.

Surescripts is committed to building relationships within the healthcare community and working collaboratively with key industry stakeholders and organizations to improve the safety, efficiency, and quality of healthcare by improving the overall prescribing process. At the core of this improvement effort is a healthcare infrastructure that establishes electronic communications between pharmacists, prescribers, and payers, and which enables the two-way electronic exchange of prescription and prescription related information.

Surescripts does not develop, sell, or endorse specific electronic prescribing software. Instead, Surescripts works with (i) software companies that supply electronic health record (EHR) and electronic prescribing applications to physician practices, (ii) pharmacies that have their own proprietary systems and pharmacy technology vendors that supply their information management systems to pharmacies, and (iii) payers and PMBs, all in order to connect their solutions to the infrastructure operated by Surescripts. Technology vendors and payers cannot connect to Surescripts unless and until they complete a comprehensive certification process. As part of its certification process, Surescripts establishes ground rules that safeguard the fairness of the prescribing process, including rules that, among other things, ensure patient choice of pharmacy and physician choice of therapy.

On a technical level, the certification process specifies the standard technical formats for transmitting prescription and related information and tests each vendor's electronic connections to the network. The formats are based on the NCPDP SCRIPT and Formulary and Benefits standards, which are consistent with the requirements of the Medicare Modernization Act of 2003 and implementing regulations. The certification rules also ensure that prescribing decisions are based on best medical practices, not on financial considerations or the interests of one particular entity. For instance, by

prohibiting commercial messaging to prescribers at the point of prescribing, Surescripts is helping to safeguard the fairness and appropriateness of the prescribing process.

Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

We are concerned that HHS' guidance contemplates a rigid framework which provides an "exhaustive list of technologies and methodologies." We would recommend a more flexible approach, and an approach that takes into account both the various entities that will serve as Covered Entities and Business Associates for purposes of storing and exchanging PHI as well as new and developing technologies and methodologies. Our concern regarding this rigid approach manifests itself in the reference to NIST SP800-111 for the storage of encrypted information. It is our interpretation of NIST SP800-111 that it applies only to end user devices, and not, for instance, the kinds of servers and systems that we employ at Surescripts. NIST SP800-111 is not relevant for the server-class computers that many organizations use in their data centers. Accordingly, one could argue that no business associate intermediary such as Surescripts would be able to avail itself of the safe harbor protection regarding compliance with the breach notification requirement. We do not believe that such a result is the intent of HITECH. We would recommend any of these encryption algorithms be considered and incorporated into this Guidance:

- AES
- 3DES, RC4
- SHA1

We are concerned that HHS' guidance appears to undo the HIPAA Security Rules by the designation of specific technologies to the exclusion of all other technologies and methodologies. If HHS designates certain technologies and methodologies as safe, then others, by implication, are not adequate. HHS' rigid guidance creates a *de facto* standard, rendering the flexible Security Rules meaningless. Ultimately, this will create a security regimen that is actually less secure, as a rigid standard does not consider necessary allowances for various types of health care practices and environments.

We ask HHS to expand the guidance to include a flexible approach as envisioned by the HIPAA Security Rules, which is the regimen under which covered entities have been operating for a number of years.

Definition of Breach

Section 13400(1) of the Act defines a breach as unauthorized acquisition, access, use or disclosure of PHI, which compromises the privacy or security of such information. This is a very broad and expansive definition. In HHS' upcoming rules, we ask that HHS provide necessary clarification of this definition. For instance, consider the circumstance of a provider sending a patient record to another provider in the good faith belief that such receiving provider is the patient's current provider of care. In some circumstances, the patient may in fact not be receiving services from that receiving provider. It would appear that this would be considered a breach even though the access was in good faith and not likely to result in any patient harm. We suggest that HHS consider such facts and circumstances in providing guidance as to what would constitute a breach.

Exceptions to the Breach Definition

Under the HITECH Act, there are exceptions to the breach definition. We ask HHS to provide clarification with respect to these exceptions. The first exception is where an unauthorized person to whom information was disclosed would not reasonably have been able to retain the information. We believe that appropriate examples of this exception would include:

- oral and telephonic disclosures, such as when information is shared with the wrong covered entity, business associate, or patient
- handing information to the wrong patient and the error is corrected before the patient leaves the premises

Under these examples, PHI may have been disclosed, but it is not reasonable to expect that the recipient would be in a position to retain any PHI.

Breach Notification

Section 13402(c) of the HITECH Act provides when a breach must be treated as "discovered" for the purposes of the Act. With respect to breach discovery, we ask HHS to consider FTC's proposed provision in which FTC recognizes that certain breaches may be very difficult to detect, and that an entity with strong breach detection measures may fail to discover a breach. In such circumstances, FTC would not consider the failure to discover the breach a violation of the rule. Considering the penalties that would attach to a violation of the Act, we believe this reasonableness standard to be appropriate. So long as a covered entity has taken reasonable steps to protect PHI and discover breaches, they

should not be considered to be in violation of the rule for breaches that reasonable measures would not prevent or detect.

Under Section 13402(d), breach notifications must be made without "unreasonable delay." We agree with this reasonableness standard; however, we ask HHS to consider that when an employee alerts management about a potential breach, an investigation must be conducted to determine if a breach has, in fact, occurred. This necessary step should be included in the determination of whether any delay is reasonable.

Section 13402(d)(3) requires notification to the Secretary "immediately" if the breach was with respect to 500 or more individuals. The FTC has proposed "immediately" to not exceed five business days.[1] As mentioned above, when an employee alerts management about a potential beach, an investigation has to be conducted to determine if a breach occurred and the number of people potentially affected. We believe in many cases that five business days would not allow enough time to conduct a proper investigation, especially for large corporations with hundreds to thousands of locations. We believe a more reasonable time frame would be 60 days, the same as the time limit for notifying individuals.

The substitute notice requirement under § 13402(e)(1)(B) requires posting on the home page of the Web site of the covered entity for a period to be determined by the Secretary of HHS. With respect to the period of time for which the posting is required, we ask that HHS consider that leaving information on a Web site for an unnecessarily long period of time would lead to confusion to consumers, as they may see information about the same incident and wonder if the posting refers to the same or a newer incident. We believe that an appropriate period of time would be 60 days. We ask HHS to clarify that the posting on the home page may consist of a link to another page with more detailed information, as requiring all the information about a breach on the home page would lead to an unnecessarily cluttered and confusing home page.

The alternative form of substitute notice under § 13402(e)(1)(B) is media notice "in major print or broadcast media, including major media in geographic areas where individuals affected by the breach likely reside." The FTC's proposed rule is substantively identical to this statutory provision, but also would add "which shall be reasonably calculated to reach individuals affected by the breach."[2] We agree with FTC's assessment that because the notice is intended to serve as a substitute to particular

[1] As proposed under 16 CFR 318.5(c)
[2] As proposed under 16 CFR 318.5(a)(4)(ii)

individuals, it should be reasonably calculated to reach those individuals. We ask HHS to adopt the same standard here as proposed by FTC.

Breach Notification and Business Associates

In the FTC's proposed rules to implement the breach notification provisions of the HITECH Act, the FTC would require a third party service provider to provide notice of breach to a senior official at the PHR vendor or related entity, and to obtain acknowledgement from such official that such notice was received.[3] FTC states that the "purpose of this requirement is to avoid the situation in which lower-level employees of two entities might have discussions about a breach that never reaches senior management. It is also designed to avoid the problem of lost emails or voicemails." We ask HHS to recognize the wisdom of this provision, and to require a similar requirement for HIPAA business associates and covered entities, with one modification. Rather than requiring notification to a generic "senior official," we ask HHS to require a business associate to provide notice of breach to the covered entity's privacy officer or privacy office. This would ensure that the covered entity would be able to respond appropriately to such notice.

Specific Questions

HHS requests feedback on several questions, issued under two headings. Our responses are provided below:

A. "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals"

Questions 1-4, and 7: HHS requests comments on which specific technologies and methodologies should be included or excluded from the guidance. As mentioned above, the identification of any specific technology or methodology would cast doubt upon other technologies or methodologies. Technology is changing rapidly; any suggested technology may be obsolete prior to updates in the guidance. We recommend that HHS' guidance follow the HIPAA Security Rule, which provides for flexibility while maintaining proper security levels. Specifically, we would recommend any of the following encryption algorithms be considered and incorporated into this Guidance:

[3] As proposed under 16 CFR 318.3(b)

- AES
- 3DES, RC4
- SHA1

B. "Breach Notification Provisions Generally"

Questions 1-3: In questions 1-3, HHS asks about interaction and potential conflict with state breach notification laws. We believe that this is an area of significant concern and will cause significant confusion in the absence of guidance regarding the pre-emptive effect of HITECH. Of particular concern, for instance, is the breach notification requirement under Massachusetts law, which specifically prohibits the patient notification from including the nature of the breach and the number of residents affected.[4] We request assistance with respect to how a covered entity would comply with both the seemingly conflicting breach notification requirements of the HITECH Act and state statutes, such as Massachusetts.

Conclusion

Thank you, again, for the opportunity to comment on HHS' breach notification guidance and to provide recommendations for HHS' breach notification rulemaking. Please feel free to contact me at 703.921.2179, if we can provide further assistance.

Sincerely,

/s/ Paul L. Uhrig

Paul L. Uhrig
General Counsel, EVP Corporate Development,
& Chief Privacy Officer

[4] M.G.L.A. 93H § 3