COALITION FOR PATIENT PRIVACY

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 Independent Avenue, SW
Washington, DC 20201

Via Email

Re: HHS Guidance and Request for Information regarding technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009

We appreciate this opportunity to provide public comment on this important issue. The Coalition for Patient Privacy is the leading voice of consumer organizations and provider groups working to encourage adoption of Health IT that is consistent with patient privacy. We are a diverse, multi-partisan group united by the effort to prevent discrimination in employment and other key opportunities based on health information and to preserve the ethical basis of the health care system. We are solely accountable to consumers and patients. The Coalition works directly with consumers of all interests, beliefs, abilities and incomes to positively impact how electronic medical records are used and to ensure privacy is protected so that patients trust the healthcare system.

While we appreciate the desire to establish reasonable, workable regulations, patients' most sensitive information on earth, their health information, must be treated with the utmost caution and concern. In short, when privacy is violated the patient must be informed. **The burden to the data holder cannot trump this important protection for consumers.**

Breach Notices are absolutely critical to the public's trust in health IT systems. Breach notices inform Americans which vendors and systems to avoid and by inference which offer the highest level of protection for sensitive health data. It is essential that HHS ensure that breaches are reported in all situations the average person considers to be a

privacy or security breach. Breach notices must apply in a comprehensive rather than a narrow or selective way.

As an agency serving the public, we urge HHS to hold up the highest bar for privacy and security standards. In 2008, 7,033,064 personal health records were breached[1]. The causes of the breaches were: 4,349,087+ due to "Data on the Move", 2,241,363+ due to "Subcontractors", 12,000+ due to "Hacking", 335,805+ due to "Accidental Exposure", and 94,809+ due to "Insider" Theft. Recent research shows that new kinds of breaches of health information are not even being tracked. For example, file-sharing P2P software is causing hospital electronic health records to be exposed[2].

While a notable increase in breach notifications is rightfully frightening and potentially damaging to corporations; those consequences do not justify lax interpretation or enforcement of the federal breach notification provision. It is a well settled rule that civil statutes for the protection of the public, such as these, must be liberally construed so as to effectuate their object and purpose, and to suppress the mischief at which they are directed. **Setting the highest standards for breach reporting and requiring the encryption of PHI in transit encourages the responsible entities to improve their security and privacy protections on the front end.** Our ultimate goal is to avoid breaches of sensitive personal information altogether.

Encryption & Destruction

With regard to methods that render PHI unusable, unreadable or indecipherable to unauthorized individuals, the Coalition for Patient Privacy urges you to only allow encryption and destruction as the bare minimum methods. In fact, we encourage HHS to require the highest levels and standards of encryption for all PHI, including ensuring encryption keys are at least 128 bits in length and not stored with the encrypted data. The rule should formally state that when an encryption key has been breached or when key and data are transferred together, the information is not considered unusable, unreadable or undecipherable. In addition, we encourage HHS to require state of the art privacy and security enhancing technologies and methods such as independent consent management tools to prevent breaches in the first place.

Encryption of data in use, disposed and in motion should be required as a minimum standard, not just a measure that excludes the breach notification requirement. High levels of encryption are standard in many other business sectors that hold/transfer far less sensitive data than is used and transferred in the health care sector. For example, in Internet commerce and Voice over Internet Protocol phone services, data encryption is the standard. As such, weaker encryption or no encryption of sensitive PHI and

[1] Identity Theft Resource Center at http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml
[2] "Data Hemorrhages in the Health-Care Sector" by M. Eric Johnson at: http://fc09.ifca.ai/papers/54_Data_Hemorrhages.pdf

demographic data makes no sense. At a minimum, HHS should mandate that the health care system meet or exceed the highest encryption standards/modes used in other industries.

Limited Data Sets

The Coalition for Patient Privacy agrees with the HIPAA Privacy Rule that treats information in limited data sets (LDS) as PHI. This should not change. **We strongly disagree with broadening methods that make data unusable, etc. to include use of LDS.** There should be no safe harbor measure for entities relying on LDS to protect data.

HHS notes that LDS may be used for research purposes and that in these situations there must be a data use agreement to obligate the recipient to not re-identify the data. *If HHS has already determined that use of LDS by researchers need additional protections to ensure data is not re-identified, why would HHS consider a lower standard for hackers?* No such data agreement exists when a LDS is accessed, stolen or copied by an unauthorized user or thief. If LDS are breached, the data can be re-identified and breach notice is imperative.

With regard to concern about state breach laws only requiring notice for compromised direct identifiers, we note that the federal standard can and should be the highest national standard. With regard to concern about administrative or legal difficulties of accessing sufficient contact information of patients in a LDS, we do not have much concern. The entity using a LDS is likely a business associate of the covered entity that provided the LDS. As the covered entity is the one responsible for breach notice, this entity should have access to the additional data needed for notification.

Moreover, we urge you not to rely on the removal from the LDS either the month and day of birth (but not the year), or the last 3 digits of a 5-digit zip code as a means of securing data from being re-identification. Millions of people's records can still be re-identified using LDS even with those additional identifiers removed. Dr. Latanya Sweeney PhD has shown that with the year of birth and 5–digit zip code, .04% of Americans, 12 million people, can be re-identified[3]. Additionally, LDS include places of service, admission and discharge dates, all of which facilitate re-identification. The recommendations HHS proposes lower the risks of re-identification but do not eliminate the risks of re-identification. We recommend that the HHS standard for de-identification should be that all data must be provably de-identified. Experts like Dr. Sweeney have demonstrated methods to provably de-identify health data, so the data is reliable and still protects privacy.

[3] "Strategies for De-identifying Patient Data for Research" by Latanya Sweeney, PhD, http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.html

Finally, though the issue is not directly related to the HHS Guidance at hand, we want to address the comments in this Guidance regarding the exclusion of LDS from the accounting of disclosures requirement. The Coalition recommends that ALL disclosures of PHI, including LDS be accounted for and reported because this data is so easily re-identifiable and audit trails of disclosures are cheap and easy to do automatically. Letting consumers have a meaningful audit trail of limited data set disclosure is of critical importance to build trust in electronic systems and ensure transparency and accountability. We urge HHS to reconsider previous guidance that excludes LDS when promulgating the required new regulations for the accounting of disclosures provision in HITECH.

The Ideal Standards

The Coalition encourages HHS to consider what the average man or woman on the street would view as a privacy breach. Many patients would object to many routine disclosures allowed under HIPAA without consent for purposes of treatment, payment and health care operations. For example: the average person would view having a hospital or doctor send or sell their electronic health records to a for-profit genetic research corporation without informed consent to be a privacy breach. Most people consider having their pharmacy sell their prescription records without informed consent a privacy breach. Many patients consider it a privacy breach when one of their doctors discloses PHI to another doctor without informed consent. Only 1% of Americans want their electronic health information used for research without their consent[4]. We note the majority of public comments to the Federal Trade Commission on breach notification are demanding a right to opt out of electronic systems altogether.

The public's expectation of personal control over PHI goes back to the nation's founding. These expectations are embodied by the Hippocratic Oath, medical ethics and the very strong legal privacy rights and protections in state law, common law, tort law, Constitutional law, the physician-patient privilege, the psychotherapist-patient privilege, and the right to privacy in ten state constitutions. As we all share a common goal of encouraging adoption of Health IT, we urge HHS to take the lead in restoring and building public trust in electronic systems. One way HHS can and should lead is by expanding the definition of what constitutes a breach to include any use or disclosure of data without meaningful, informed consent.

It is critical that HHS not focus simply on encryption technologies and breach notices as the key solutions to build a trusted health IT system. The healthcare industry already perceives these two measures alone as a "silver bullet". Many in the industry think that if they use encryption they've done their part to protect private information. The

[4] "How the Public Views Privacy and Health Research, Results of a National Survey Commissioned by the Institute of Medicine Committee on "Health Research and the Privacy of Health Information: The HIPAA Privacy Rule", Original Report - November 2007; Revised and expanded - March 2008 at: http://www.patientprivacyrights.org/site/DocServer/WestinIOMSrvyRept.pdf?docID=2501

problem is that many breaches in healthcare stem from "authorized"' users who misuse their access and from unknown and untracked access to data via methods like P2P file-sharing software. Encryption will not address these other major threats to privacy.

While encryption technologies are definitely an important step, HHS should ensure that their message to the healthcare industry is clear: encryption does not absolve organizations from other technical measures and operational methods necessary to protect patients' privacy. Encryption is important but only a partial solution to the culture change needed to protect privacy. Without clear messaging, healthcare organizations are already budgeting and starting projects around encryption to the exclusion of all the other changes needed in operations and human processes.

There is no silver bullet to protecting sensitive PHI and organizations and government need to be more diligent then ever in protecting private information in the current environment of increasing threats to electronic privacy.

Responses to HHS' direct questions

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

1. Are there particular electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as a fingerprint protected Universal Serial Bus (USB) drive, which are not sufficiently covered by the above and to which guidance should be specifically addressed?

   We do not recommend granting any additional safe harbors to more media or devices without extensive testing for effectiveness and proof that data is safe and cannot be accessed. These methods/media must be fully vetted and approved by NIST. Further, we prefer that HHS recommend privacy-enhancing technologies be used such as second factor authentication, robust independent consent management tools, multiple levels of encryption, technologies to prevent spoofing, etc.

   Any fingerprint or other biometrically enabled protections should be subject to a particularly high level of scrutiny. In addition to law enforcement, many private sector entities are engaged in the widespread collection of biometrics for a variety of tasks including gym memberships, paying for school lunch, and paying for groceries. With the ease of storage and sharing of personal information it is certain that large databases of individual biometrics will emerge (to the extent that they have not already). Any security measure that relies on the security of a biometric must therefore be automatically suspect.

2. With respect to paper PHI, are there additional methods the Department should consider for rendering the information unusable, unreadable, or indecipherable to unauthorized individuals?

We recommend that all paper medical records or other kinds of medical records (such as microfiche) be shredded or destroyed at a reasonable time after the patient's death. Old records threaten the privacy of future descendants.

3. Are there other methods generally the Department should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?

HHS should instead focus on protecting our sensitive information on the front end. Require the use of privacy and security enhancing technologies to prevent breaches in the first place.

We also recommend that HHS require opt-in to the use of all electronic health systems. If an alternative paper system cannot be used when people opt-out, individuals should be allowed to block all electronic sharing of PHI outside of the single entity that holds PHI.

4. Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?

We recommend requiring the best mode or highest level of encryption for all PHI as discussed beginning on page 2. Weaker modes and lower levels of encryption mean data can be hacked more easily.

5. Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals?

YES. Please see our commentary beginning on page 3.

Can risk of re-identification be alleviated such that the creation of a limited data set could be added to this guidance?

NO. Please see our commentary beginning on page 3.

6. In the event of a breach of protected health information in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?

As noted in our commentary beginning on page 3, we do not find any administrative or legal concerns regarding compliance.

Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

YES. Specifications can provide a useful benchmark for providers, especially smaller entities that may have a limited budget for meeting privacy and IT needs. Such standards should be updated annually to assure they remain state of the art.

B. Breach Notification Provisions Generally

1. Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues the Department should consider in promulgating the federal breach notification requirements?

The federal breach notification requirements should hold the highest standard. We do not encourage any exceptions that limit what qualifies as a reportable breach. We do encourage broadening the definition of a reportable breach, consistent with the consumer concerns noted above.

2. Given current obligations under state breach notification laws, do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach? Are there circumstances in which the required federal notice would not also satisfy any notice obligations under the state law?

The Coalition would lean on the side of redundancy of notification. While it may appear alarmist to some, it is easy to miss notifications, misunderstand notifications or otherwise fail to recognize the content of a notification in these information-laden "junk mail" times. Further, for people with disabilities, one notification may be insufficient for any number of reasons, particularly if it is not available in an alternate format, such as for those with vision loss.

Further, there are many other reasons why redundancy of contact about a breach would be helpful, including circumstances in which a person lives in congregate settings, where mail may be slow or misdirected, when caregivers or representatives are used that routinely handle business affairs on a monthly or biweekly basis, when PO Boxes are used due to transitory life-styles, or when living in multiple locations (home, disability setting, rehab hospital or other treatment location). These circumstances could easily lead to delay of receipt of notification. In such situations, redundancy of contact about a breach is a plus as it increases the chance patients will learn of the breach and be able to take any

necessary steps to stanch any likely damage or prompt them to have someone else take the necessary steps.

3. Considering the methodologies discussed in the guidance, are there any circumstances in which a covered entity or business associate would still be required to notify individuals under state laws of a breach of information that has been rendered secured based on federal requirements?

No comment.

4. The Act's definition of "breach" provides for a variety of exceptions. To what particular types of circumstances do entities anticipate these exceptions applying?

We do not encourage any exceptions. The patient is always the best person suited to determine if a "breach" is unauthorized or malicious.

Additional Recommendations and Comments:

- We encourage HHS to adopt a number of the provisions from the Federal Trade Commission (FTC) regulations. Specifically, the "presumption of breach" language that puts the onus on the health care entity to prove that they information was not accessed is needed here. HHS guidance would also benefit from incorporating the FTC's very useful clarification of exactly what identifiable health info is.

- We encourage HHS to include Guidance on the form of breach notification and include requirements that the notice be available in alternate formats such as large fonts, Braille and audiotape at the request of the patient effected. Registering these preferences should be built in to electronic record keeping systems.

- We support the requirement that covered entities and business associates that do a bad job of protecting PHI should be identified and listed as required by statute when their systems are breached.

- We propose that the IT vendors of systems/products that are breached be identified and reported in the same way that covered entities and business associates are reported. This transparency and accountability measure will assist providers in selecting the right vendor.

- To further enhance transparency of this process, we request that HHS release the log of meetings with and names of the external experts in health informatics

and security that it consulted with to develop this guidance and publish all materials and documents provided by these consultants.

- All experts consulted should be required to disclose all conflicts of interest in writing.

Conclusion

Ironclad protection against theft and misuses of PHI must be the price of doing business in health care. If an entity cannot or will not protect our most sensitive data, they should not be in the health care business. We currently have higher standards and expectations for our financial data than we do for our health data. With a breach of financial records, a consumer faces a significant headache, but ultimately can have their credit and funds restored; this is not the case with health records. A stigmatizing diagnosis, condition or prescription in the wrong hands can cause irreversible damage and discrimination. There is no perfect delete or recover button for Health IT.

The burden to the data holder cannot trump this important protection for consumers. The Coalition urges HHS to hold the highest standards for breach notification. Thank you for this important opportunity to provide feedback on this guidance and request for information.

Sincerely,

The Coalition for Patient Privacy

American Association of People with Disabilities
American Civil Liberties Union
Clinical Social Work Association
Confederation of Independent Psychoanalytic Societies
William duSold, Individual
Electronic Frontier Foundation
JustHealth
Patient Privacy Rights
Privacy Journal
Private Citizen, Inc.
The Privacy Professor
The Multiracial Activist
National Association of Social Workers
The National Coalition of Mental Health Professionals and Consumers
U.S. Bill of Rights Foundation