Appendix 1

patientprivacyrights

May 18, 2010

Office of Civil Rights
Department of Health & Human Services

Re: HIPAA Privacy Rule Accounting of Disclosures Under the HITECH ACT: Request for Information (Doc ID HHS-OCR-2010-0009-0001)

II. Questions

1. What are the benefits to the individual of an accounting of disclosures, particularly of disclosures made for treatment, payment, and health care operations purposes?

An accounting of disclosures of protected health information (PHI) is critical to building patient trust in electronic healthcare systems. Patients cannot presently control the use of PHI in electronic health systems since no consent is required for uses of PHI for treatment, payment and health care operations. As such, an accounting of all disclosures would enable greater transparency and accountability for the use of PHI.

Individuals would prefer to "own" and control their PHI in electronic systems, according to the AHRQ:

- A majority want to "own" their health data, and to decide what goes into and who has access to their medical records (AHRQ p. 6).
- A majority believes their medical data is "no one else's business" and should not be shared without their permission. This belief was expressed not necessarily because they want to prevent some specific use of data but "as a matter of principle". (AHRQ p. 18)[1]

Currently, there is no accountability and transparency in HIT systems and far beyond healthcare as PHI flows unbounded to secondary and tertiary entities. Informed

[1] AHRQ Publication No. 09-0081-EF "Final Report: Consumer Engagement in Developing Electronic Health Information Systems" Prepared by: Westat, (July 2009) See: http://healthit.ahrq.gov/sites/default/files/docs/activity/consumer_engagement_in_developing_electronic__2009_update_2.pdf

consent is not required for each new use of data. According to Latanya Sweeny, in her testimony at a recent congressional briefing[2]:

- "Since the passage of HIPAA, there has been an explosion in the collection and sharing of patient information. While HIPAA explicitly identifies covered entities that handle patient information, **there is no identification of the vast number of business associates who receive patient information from covered entities, or of the business associates of those business associates, and so on, as secondary sharing is unbounded. Data sharing through business associate arrangements is widespread yet hidden from patients, making harms difficult to trace."**
- **"Having meaningful users of EMRs (electronic medical record systems) as encouraged by ARRA [6] will further increase data sharing, but the most dramatic increase will be a consequence of benefits made possible by nationally sharing patient information over the NHIN."**

Congress' intent to require an accounting of disclosures was to provide individuals with accountability and transparency of the use of their sensitive health information so they could know who accessed, used, or disclosed their PHI. The expansion in data sharing when certified EHRs are in widespread use and the proposed NHIN models are working, will vastly expand data sharing as Dr. Sweeney pointed out. Without meaningful audit trails, all of those uses and disclosures would remain hidden from patients, making the HIT system neither accountable nor transparent.

Patients expect to know how their PHI is used and for what purposes. If they cannot find out how their information was shared, with whom, and for what purposes, one in eight will either refuse treatment or refuse to fully communicate with providers[3], which will undermine electronic health information exchange generally resulting in erroneous and incomplete data. There is no way to trust HIT systems if you have no control over where your PHI flows and no accounting of disclosures.

2. Are individuals aware of their current right to receive an accounting of disclosures? On what do you base this assessment?

---

[2] The Congressional briefing on April 22nd was a roundtable discussion on the "Implementation of Health Information Technologies in a Healthcare Environment". The briefing was hosted by Representatives Patrick Kennedy and Tim Murphy and sponsored by the Capitol Hill "Steering Committee on Tele-health and Healthcare Informatics" and the Institute for e-Health Policy. See: http://patientprivacyrights.org/wp-content/uploads/2010/04/Sweeney-CongressTestimony-4-22-10.pdf

[3] See National Consumer Health Privacy Survey 2005, Conducted for the California HealthCare Foundation by Forrester Research, Inc. November 9, 2005

Generally speaking, individuals are not aware of their right to an accounting of disclosures. We have contact with many individual consumers through our website along with technology experts and have not come across anyone aware of their current right to receive an accounting of all non-TPO disclosures. The non-TPO disclosures are rare since by far the most uses and disclosures of PHI are for TPO. The current right to an accounting of non-TPO disclosures appears not to be explained to patients.

If patients were more aware of how often their information is being inappropriately shared with people who have no direct relationship with them, they would likely want to have more information about their rights to an accounting of disclosures, so they could exercise it.

3. If you are a covered entity, how do you make clear to individuals their right to receive an accounting of disclosures? How many requests for an accounting have you received from individuals?

We are not a covered entity, but the leader of the bipartisan Coalition for Patient Privacy representing over 10 million Americans. The individuals we represent have long advocated for a full accounting of all uses and disclosures of PHI for TPO. This right needs to be communicated to patients in clear, user-friendly ways. Best practices would indicate both oral and written notification.

4. For individuals that have received an accounting of disclosures, did the accounting provide the individual with the information he or she was seeking? Are you aware of how individuals use this information once obtained?

Patient Privacy Rights has not been contacted by any consumers who have received and accounting of non-TPO disclosures. Again, since the vast majority of disclosures fall under TPO, we would be surprised if the previous non-TPO only accounting right would reveal anything meaningful to the individual.

5. With respect to treatment, payment, and health care operations disclosures, 45 CFR 170.210(e) currently provides the standard that an electronic health record system record the date, time, patient identification, user identification, and a description of the disclosure. In response to its interim final rule, the Office of the National Coordinator for Health Information Technology received comments on this standard and the corresponding certification criterion suggesting that the standard also include to whom a disclosure was made (*i.e.,* recipient) and the reason or purpose for the disclosure. Should an accounting for treatment, payment, and health care operations disclosures include these or other elements and, if so, why? How important is it to individuals to know the *specific* purpose of a disclosure—*i.e.,* would it be sufficient to describe the purpose generally (*e.g.,* for ''for treatment,'' ''for payment,'' or ''for health care operations purposes''), or is more detail necessary for the accounting to be of value? To what extent are individuals familiar with the different activities that may constitute ''health care operations?'' On what do you base this assessment?

The bipartisan Coalition for Patient Privacy's member organizations believe that an accounting of disclosures should include all the specific elements listed above, otherwise individuals have no meaningful information about who has seen or used their PHI, or why. The right to an accounting of disclosures has to include critical details such as 'who' i.e., which actual person(s) actually receive, use, or disclose PHI and the specific purpose or reason for each use or disclosure. "Treatment" and "payment" are specific reasons or purposes, but "health care operations" is far too broad a category of use to be transparent or comprehensible to individuals.

Every specific type of health care operations use should be spelled out specifically, such as "use and/or disclosure of data for quality improvement about the use an antibiotic(s) taken by the individual", or "use and disclosure of data to evaluate the comparative effectiveness of treatments for diabetes (or depression, etc)", or the "use and/or disclosure of data for population-based studies on obesity", or the "use and/or disclosure of data for research by Pfizer on side-effects of an antidepressant you were taking", or the "use and/or disclosure of data for sale to a specific research corporation studying x, y, or z". HCO is such broad category that exposes patient data to such great risks, that it requires very comprehensive specification of purpose and data users (i.e., specific named persons employed by each provider or covered entity or business associate should be provided).

We find frequently that experts in technology and healthcare are not familiar with the many possible uses of PHI covered under "health care operations", and the general public is even less aware of what HCO means. The uses and disclosures of PHI for TPO will require meaningful public education.

6. For existing electronic health record systems: (a) Is the system able to distinguish between ''uses'' and ''disclosures'' as those terms are defined under the HIPAA Privacy Rule? Note that the term ''disclosure'' includes the sharing of information between a hospital and physicians who are on the hospital's medical staff but who are not members of its workforce. (b) If the system is limited to only recording access to information without regard to whether it is a use or disclosure, such as certain audit logs, what information is recorded? How long is such information retained? What would be the burden to retain the information for three years? (c) If the system is able to distinguish between uses and disclosures of information, what data elements are automatically collected by the system for disclosures (*i.e.,* collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the disclosure? (d) If the system is able to distinguish between uses and disclosures of information, does it record a description of disclosures in a standardized manner (for example, does the system offer or require a user to select from a limited list of types of disclosures)? If yes, is such a feature being utilized and what are its benefits and drawbacks? (e) Is there a single, centralized electronic health record system? Or is it a decentralized system (*e.g.,* different departments maintain different electronic health record systems and an accounting of

disclosures for treatment, payment, and health care operations would need to be tracked for each system)? (f) Does the system automatically generate an accounting for disclosures under the current HIPAA Privacy Rule (*i.e.,* does the system account for disclosures other than to carry out treatment, payment, and health care operations)? i. If yes, what would be the additional burden to also account for disclosures to carry out treatment, payment, and health care operations? Would there be additional hardware requirements (*e.g.,* to store such accounting information)? Would such an accounting feature impact system performance? ii. If not, is there a different automated system for accounting for disclosures, and does it interface with the electronic health record system?

We strongly urge OCR to keep protecting individuals' rights front and center throughout this process. It would be a mistake to implement this key privacy protection by accommodating the HIT vendor industry, which has been fighting every new consumer protection in HITECH. The accounting of disclosures is one of the KEY, CRITICAL new consumer privacy protections in the HITECH. We hope that OCR will avoid a path that helps industry justify their opposition to new consumer protections and rights. Individual Americans need the OCR to make sure industry complies with the new consumer protections.

The limitations in current HIT systems that prevent full and detailed compliance with the requirements in HITECH are minor. Authentication of all users of EHRs and HIT systems is required, so every employee access to every record or piece of PHI is already logged. The login process could be updated to require specific purpose or use, whether it was a "use" or "disclosure" and each user is already known to hospital HIT systems as a physician or employee. Part of the process of initially authenticating a user requires categorizing who has which "role" in the hospital, so generating those details automatically would not be a complex or expensive update.

With regard to the burden of data retention, that burden is minimal. The cost of data storage is so cheap now, it should not be accepted as a "burden"—in fact hospitals and providers should view retaining accounting of disclosure data as a way to assure patients their systems are transparent and accountable. Providing the most robust consumer protections could be a positive way for hospitals and covered entities to demonstrate to the public that they want to be trusted and protect consumers' interests.

Here, it seems that OCR is asking the wrong questions. Rather than asking about "what would be the additional burden to also account for disclosures to carry out treatment, payment, and health care operations?", OCR should be asking instead exactly how quickly existing EHR/HIT systems can comply with the new consumer protections and specifically justify the time and costs to upgrade the system(s).

Obviously HIT upgrades take time and there is always some cost associated with upgrades, but these costs for accounting of disclosures should be minimal. In fact, many proprietary HIT companies have already sold and implemented new products that offer

detailed accounting of disclosures. There is no reason NOT to require robust accounting of disclosures right away, because the information from the process of authentication and user access to EHR systems has most of the needed data already. It would not be hard to tweak the authentication process to add a few more data fields for users to fill in detailed purpose for use/disclosure, etc.

One example is of a robust accounting of disclosure is offered by Imprivata (there are many other authentication technology firms that have similar products):

Imprivata's PrivacyAlert™ Detects Snooping and Identity Theft:

- detects snooping, identity theft and inappropriate access
- automated and scalable privacy monitoring
- investigate and report data breaches
- investigate employees, patients or both
- Out-of-the-box supports all leading healthcare applications---Eclipsys, GE Centricity Enterprise, MEDITECH Magic, Siemens Invision, etc

See: http://www.marketwire.com/press-release/Imprivatas-New-Product-Helps-Hospitals-Proactively-Investigate-Audit-Access-Patient-1123908.htm

7. The HITECH Act provides that a covered entity that has acquired an electronic health record after January 1, 2009 must comply with the new accounting requirement beginning January 1, 2011 (or anytime after that date when it acquires an electronic health record), unless we extend this compliance deadline to no later than 2013. Will covered entities be able to begin accounting for disclosures through an electronic health record to carry out treatment, payment, and health care operations by January 1, 2011? If not, how much time would it take vendors of electronic health record systems to design and implement such a feature? Once such a feature is available, how much time would it take for a covered entity to install an updated electronic health record system with this feature?

See answers to #6. The authentication technology providers have already re-purposed the data they collect to turn it into audit trails for the accounting of all disclosures. Since all HIT systems and EHRs require robust authentication, there is no reason to delay this requirement beyond 2011. Again, the features are available and being used in the marketplace right now.

8. What is the feasibility of an electronic health record module that is exclusively dedicated to accounting for disclosures (both disclosures that must be tracked for the purpose of accounting under the current HIPAA Privacy Rule and disclosures to carry out treatment, payment, and health care operations)? Would such a module work with covered entities that maintain decentralized electronic health record systems?

There is no need for a module dedicated exclusively to accounting for disclosures. See Answers to #6 and #7. Whether systems are centralized or decentralized every user of every system has to be authenticated, so this is an odd question. Perhaps OCR is concerned about how users of HIEs or HIOs will be authenticated. Every system

requires the authentication of individuals-----large entities like hospitals must be authenticated too (like your check shows both your individual account number and the branch bank's routing number). In RHIOs, HIEs, HIOs, and NHINs, there must be an accounting of disclosures that shows both the name of entity and the name of the employee(s) or user(s).

9. Is there any other information that would be helpful to the Department regarding accounting for disclosures through an electronic health record to carry out treatment, payment, and health care operations?

OCR should make a sustained effort to meet as often with legitimate consumer, patient, and privacy advocates (ie especially those with actual members, as opposed to 'think tanks' with no members) as it does with industry.

Sincerely,

Deborah C. Peel, MD
Founder & Chair

dpeelmd@patientprivacyrights.org
(512) 732-0033

APPENDIX 2

patientprivacyrights

August 1, 2011

Georgina Verdugo
Director, Office of Civil Rights

United States Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHS Bldg.
Washington, D.C. 20201

Re: RIN: 0991-AB62

Dear Director Verdugo:

Patient Privacy Rights (PPR) is the leading national consumer voice for building ethical, trustworthy HIT systems. We have 12,000 members in all 50 states and also represent 10.3 million Americans through our leadership of the bipartisan Coalition for Patient Privacy (see: http://patientprivacyrights.org/coalition-patient-privacy/). We seek to restore the right of consent and the right to health information privacy in electronic health systems and data exchanges. Consent and control are imperative for patients to be willing to participate in electronic health systems and data exchanges.

We promote privacy-enhancing technologies (privacy-by-design) to ensure patients can move the right personal information to the right person at the right time -- while preventing unwanted sale and misuse of protected health information (PHI) by strangers we have no relationship with.

As a voice for patients, PPR has no conflict of interest, financial or otherwise. We are deeply invested in this long term process and are eager to help HHS ensure both progress and privacy. The Coalition urged Congress to include historic new privacy and security rights in the Health Information Technology for Economic and Clinical Health (HITECH) Act.[4] These core protections are essential building blocks for privacy and HIT and must be fully implemented and enforced.

[4] See our letter to Congress at: http://patientprivacyrights.org/media/CoalitionPatPriv_Final01.14.09.pdf

It is important to start with the fact that health information privacy is very important to a significant minority of the public. At the recent first-ever Summit on the Future of Health Privacy[5] in Washington, DC, legal scholar and privacy expert Alan Westin gave a keynote presentation titled, "What Two Decades of Surveys Tell Us About Privacy and HIT Today"[6]. The surveys affirm that **35-40% of the public is "Health Privacy Intense".** The "Health Privacy Intense" are:

- "Distrustful about many government and business data practices, especially if through technology systems"
- "Worried about secondary uses of their personally-identified health data, by insurers, employers, government programs"
- "Also concerned about researchers getting access to their personal health data without notice and direct consent"
- "Strongest concern: discrimination against persons with potentially stigmatizing conditions"
- "Not impressed by voluntary practices -- want legal controls and strong regulatory enforcement"
- ***"While the Privacy Intense in general consumer privacy areas are about 25%, health privacy raises this to 35-40%"***

The expectations and rights of this very significant minority of the public are not addressed by the NPRM, which violates key privacy protections in HITECH. Congress intended patients to have robust, detailed Accounting of Disclosures of PHI (AODs) by all Covered Entities (CEs) and all Business Associates (BAs) and did not restrict the AODs to information only from certified EHRs, narrow the reporting of disclosures, or exclude any CEs or BAs from providing AODs for breaches, required public health disclosures, or any other disclosures exempted in this NPRM. The point is that Congress intended patients to know where their PHI went. Congress wanted patients to have AODs that cover all PHI in HIT systems and data exchanges, not some PHI in some places. It is also critically important that patients be able to receive AODs from health information exchanges (HIEs), health information organizations (HIOs) and all other types of data exchanges.

This NPRM is the third time that HHS has proposed regulations that violate the federal statute HHS was supposed to implement. The first instance occurred when HHS eliminated the right of consent in the Amended Privacy Rule on 2002; the second was the introduction of a "harm" standard for breach reporting, which Congress specifically rejected during its own

[5] See http://www.healthprivacysummit.org/

[6] See slides from Westin's presentation at the summit at: http://patientprivacyrights.org/wp-content/uploads/2011/06/AFW-SUMMIT-6-13-11.pdf.

deliberations[7]. This is the third time HHS has violated statutory protections by weakening the strong requirements for AODs Congress intended to provide via regulations.

The history of the AOD requirement in HITECH is important

If HHS does not require robust and complete accounting of all disclosures of PHI, as Congress intended, patients in the US will not know where their data flows, who sees it, or how it is used (purpose). The healthcare system will have no accountability or transparency, and at least 35-40% of the public already do not trust electronic systems. Knowing about all uses, disclosures, and access to our PHI is particularly critical in today's systems because HHS eliminated Americans' longstanding legal and ethical rights to decide who can see and use our PHI in 2002. HHS amendments to HIPAA violated Congress' intent to provide a federal right to privacy and consent:

- *"The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."* [8]

The resulting lack of health privacy causes many millions of people in the US to avoid treatment for cancer, mental illnesses, addiction, and sexually transmitted diseases every year (see HHS' figures on page 7 in "The Case for Informed Consent" by Deborah C. Peel, MD and Ashley Katz, August 31, 2010[9]).

Patients refuse treatment and omit sensitive data when they know treatment records are not private. These are very significant unintended consequences that worsen the quality and effectiveness of healthcare. It is very significant fact that millions of patients actually put their lives and health at risk because they know their health data will be exposed and disclosed without their consent.

Further, today there is no accountability and transparency in HIT systems or far beyond healthcare where PHI flows unbounded to secondary and tertiary entities. Informed consent is not required for each new use of data, so Robust AODs are essential. According to Latanya Sweeny, in her testimony at a congressional briefing last year[10]:

---

[7] In the October 1, 2009 letter to HHS Secretary Sebelius, the Chairmen of the House Energy & Commerce and House Ways & Means Committees confirmed that the harm standard contradicted Congressional intent. Committee members *"specifically considered and rejected such a standard due to concerns over the breadth of discretion that would be given to breaching entities, particularly with regard to determining something as subjective as harm from the release of sensitive and personal health information."*

[8] 67 Fed. Reg. 53,183

[9] http://patientprivacyrights.org/2010/08/the-case-for-informed-consent/

[10] The Congressional briefing on April 22nd was a roundtable discussion on the "Implementation of Health Information Technologies in a Healthcare Environment". The briefing was hosted by Representatives Patrick Kennedy and Tim Murphy and sponsored by the Capitol Hill "Steering Committee on Tele-health and Healthcare Informatics" and the Institute for e-Health Policy. See: http://patientprivacyrights.org/wp-content/uploads/2010/04/Sweeney-CongressTestimony-4-22-10.pdf

- "Since the passage of HIPAA, there has been an explosion in the collection and sharing of patient information. While HIPAA explicitly identifies covered entities that handle patient information, **there is no identification of the vast number of business associates who receive patient information from covered entities, or of the business associates of those business associates, and so on, as secondary sharing is unbounded. Data sharing through business associate arrangements is widespread yet hidden from patients, making harms difficult to trace."**

- **"Having meaningful users of EMRs (electronic medical record systems) as encouraged by ARRA [6] will further increase data sharing, but the most dramatic increase will be a consequence of benefits made possible by nationally sharing patient information over the NHIN."**

Congress' intent to require an accounting of disclosures was to provide individuals with accountability and transparency about the use of their sensitive health information; they could know who accessed, used, or disclosed their PHI. When certified EHRs are in widespread use and the proposed NHIN models are working data sharing will vastly expand, as Dr. Sweeny pointed out. Without meaningful AODs, all of those uses and disclosures would remain hidden from patients, making the HIT system neither accountable nor transparent. Requiring business associates (BAs) to produce AODs and include them in the AODs provided by covered entities (CEs) is a significant improvement that will add more transparency and accountability to healthcare.

Patients expect to know how their PHI is used and for what purposes. If they cannot find out how their information was shared, with whom, and for what purposes, more than one in eight will either refuse treatment or refuse to fully communicate with providers[11], undermining electronic health information exchange and resulting in erroneous and incomplete data. "Treatment" and "payment" are specific reasons or purposes for disclosing PHI, but "health care operations" is far too broad a category of use to be transparent or comprehensible to individuals. Purposes must be specific. Many more patients won't trust HIT systems if the accounting of disclosures is narrowed, and if the purpose is not required.

Congress intended for patients to have a full, detailed accounting of the uses and disclosures of all PHI because the Amended HIPAA Privacy Rule eliminated patients' consent and control over the use and disclosure of PHI for routine purposes. Therefore, Congress wrote very strong, clear language in HITECH requiring robust, detailed AODs to enable transparency and accountability instead of narrowing the definition of Healthcare Operations (HCO). The bipartisan Coalition for

[11] See National Consumer Health Privacy Survey 2005, Conducted for the California HealthCare Foundation by Forrester Research, Inc. November 9, 2005

Patient Privacy was the key consumer coalition pressing for robust accounting of disclosures in HITECH (see our letter to Congress about HITECH[12]).

Another problem posed by not requiring the purpose for disclosures or access is Congress intended that consumers who pay for treatment out-of-pocket can restrict the use and disclosure of PHI to health plans and insurers. If AODs do not include the purpose of the use or disclosure then when CMS audits CEs and BAs, or when patients receive AODs, neither will be able to tell if patients' rights to restrict the flow of data were honored or violated by a CE or BA.

The failure to record the purpose of a disclosure will also impede the ability of the Office of Civil Rights and law enforcement to determine whether a violation of the HIPAA and HITECH laws was due to "reasonable cause" or "willful neglect" which makes a significant difference in the penalties that are to be assessed. Not knowing the purpose of a use or disclosure will make it impossible to assess "willful neglect" by CEs and BAs, making it impossible to assess compliance with HITECH's new patient rights and protections.

The Coalition and other consumer organizations pressed for these provisions so patients can understand what happens today to their PHI in electronic health systems and data exchanges. Unfortunately HHS did not require patients' longstanding legal and ethical rights to control and segment data in the "Meaningful Use" regulations or other new regulations, even though Congress intended HIPAA to be the "floor" for privacy rights, not the "ceiling". Congress intended that more stringent privacy protections in state and federal law, in common and Constitutional law, and in medical ethics would prevail over weaker HIPAA privacy protections.

- As HHS stated in issuing the Amended Rule: "The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order to not interfere with such laws [affording a right of consent] and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a 'best practices' standard. Thus, professional standards that are more protective of privacy retain their vitality.[13]"

In addition, without full, robust, and clear AODs, the US could experience the same kind of public rejection of HIT and data exchange witnessed in the United Kingdom. When the UK decided to add PHI to the National Health data base without patient consent there was a public outcry.[14]

---

[12] See our letter to Congress at: http://patientprivacyrights.org/wp-content/uploads/2013/08/CoalitionPatPriv_Final01.14.091.pdf

[13] 67 Fed. Reg. at 53,212 (August 14, 2002).

[14] See: UK Telegraph, Controversial medical records database suspended. A controversial scheme to upload confidential medical records to a national database has been suspended following public outcry, Kate Devlin, Medical Correspondent, 17 Apr 2010 at: http://www.telegraph.co.uk/health/healthnews/7598520/Controversial-medical-records-database-suspended.html

- The project triggered anger when it was revealed that information could have been logged on the system without patients' knowledge.

- The British Medical Association (BMA) warned that many people were not even aware of the scheme, let alone the fact that they could 'opt out'.

AODs for Research and Public Health Use and Disclosure of PHI, the HIPAA "Research" and "Public Health" Loopholes

We recognize that the IOM and many respected scientific and research institutions believe that many kinds of researchers, public health authorities, quality improvement organizations, patient safety organizations, and epidemiologists should have open access to PHI without patient knowledge or consent and believe that obtaining patient consent is a burden. They oppose AOD requirements.

Unfortunately, the public wants to know about and prefers to give consent for all research, public health, quality improvement, biosurveillance, patient safety, pay-for performance, comparative effectiveness research, and epidemiology and population health uses of PHI. The IOM's lack of support for AODs is short-sighted. Legitimate researchers, public health authorities, and epidemiologists should recognize that one of the main ways PHI flows out of the healthcare system to secondary and tertiary users for data sales and misuse is via the "research" and "Public Health" loopholes in HIPAA. They should support AODs and access reports so that patients can learn when and how their data is being used legitimately for research and not conflate the use of PHI for business analytics by for-profit corporations with legitimate research and public health uses of PHI that actually benefit patients by improving health, healthcare quality, and lowering costs.

Further, the public strongly opposes unfettered research access to PHI. Alan Westin's survey for the IOM in 2008 on the effects of the HIPAA on research[15] found:

- Only 1% of the public agreed that researchers would be free to use personal medical and health information without consent

- Only 19% of the public agreed that personal medical and health information could be used as long as the study "never revealed my personal identity" and it was supervised by an Institutional Review Board.

Unfortunately the IOM, most researchers, and HHS ignore Westin's findings.

---

[15] Westin/Harris Survey for the Institute of Medicine, Results of a National Survey, on "Health Research and the Privacy of Health Information: The HIPAA Privacy Rule" by Dr. Alan F. Westin, See: http://patientprivacyrights.org/media/WestinIOMWkshp2-28-08.ppt

Mark Rothstein[16] concluded that the IOM "missed the mark" when it recommended open access to PHI without consent for research purposes.

He wrote, "Clinicians, researchers, and their institutions do not have the moral authority to override the wishes of autonomous agents. Individuals seeking treatment at a medical facility are not expressly or impliedly waiving their right to be informed before their health information and biological specimens are used for research. The recommendation of the IOM Report would automatically convert all patients into research subjects without their knowledge or consent".

Even more troubling than the lack of concern about the public's attitudes toward research on PHI without consent is the fact that the legitimate clinical and academic research communities and public health authorities do not acknowledge the commercial exploitation of the "research" and "public health" loopholes by for-profit health "research" corporations[17], such as prescription data mining corporations, insurers, hospitals, labs, pharmacies, and technology and hardware vendors.

The existence of a large commercial "research" industry whose "research" does nothing to improve health or benefit patients will blacken the reputation of the legitimate research community, blacken the reputation of public health authorities, and cause a loss of faith in healthcare professionals and government for not protecting patients' rights to health information privacy. Commercial use and sale of PHI for corporate business analytics and data analyses will corrode patient trust in legitimate research and public health uses of PHI. This difficult problem cannot be solved by denying it exists or by re-defining "research" and "public health" data uses to exclude commercial "research and public health" use of PHI. This destructive situation makes robust AODs and access reports essential for public trust. Without the right of consent and control over data, transparency for all uses and disclosures is mandatory for the accountability of electronic healthcare systems and data exchanges.

Public health access to medical records and PHI has always been granted by statutes that address specific diseases such as TB, HIV/AIDS, SARS, etc. The public has never debated or agreed to unlimited access to medical records or PHI without consent by public health agencies. Congress did not consider that the "Public Health" loophole would result in a massive expansion of the mission and definition of public health. This expansion has never been debated, much less endorsed by the public. The history of public health is a story of vigorous public debate over the collection and use of health information about specific infectious diseases, leading to public consensus and lawmaking that addressed specific threats posed by deadly infectious diseases. Public consensus on the collection of personal health information was built disease by specific disease, threat by threat. Public health authorities and the government have never sought,

---

[16] "Improve Privacy in Research by Eliminating Informed Consent?" IOM Report Misses the Mark. In The Journal of Law, Medicine & Ethics, Volume 37, Issue 3 (p 507-512) by *Mark A. Rothstein.* See: http://patientprivacyrights.org/wpcontent/uploads/2010/02/Rothstein-ReIOM-Report.pdf

[17] See Evidence of Disclosure, The Sharing, Selling, Re-selling and Unauthorized Use of our Personal Health Information: Identifiable Data, "De-identifiable Data", and Why it Matters, compiled by Patient Privacy Rights: http://patientprivacyrights.org/media/Evidence_of_Disclosure.pdf

much less achieved public support for unlimited use of PHI for any problems public health authorities seek to affect. The consequence must be transparency and accountability of all public health uses of PHI, because these expanded uses are not known to the public.

Further, HHS has ignored the fact that informed consent is required for "research" and "public health" uses of PHI by ethical codes for research[18] and by international treaty[19]. Patients will avoid treatment, out of fear that their health information will be used for research or public health uses they do not support. Many religious people object to the use of their health information for research about certain conditions they find objectionable. The ethical codes of all health professions require informed consent before use or disclosures of personal health information[20].

"The well- being of the human subject should take precedence over the needs and interests of society."[21]

News stories confirm that the public is not willing to have sensitive personal health information, such as genetic information, used or sold without consent. Texas parents were very upset to find out that the State of Texas sold their newborn's bloodspots for research without their consent[22]. The Havasupai Indians of New Mexico sued researchers at Arizona University for using their blood for genetic studies of schizophrenia without their permission[23].

Recently Kaiser Permanente announced the development of a new research data base of 100K EHRs with genomic records. But instead of using the existing Kaiser Permanente HIT system for robust email communication with patients to obtain informed consent for the use of PHI for a specific research project or specific categories of research, Kaiser Permanente decided to use blanket advance consent for all research uses of the data base.[24] It is puzzling that Kaiser Permanente made this choice when it could have easily empowered patients to set up a broad array of personal directives to consent to approved research uses and contacted them electronically for any exceptions or new uses not covered by their personal directives.

If Kaiser Permanente does not permit patients to give consent for research on their data, shouldn't those patients be able to see all research uses and disclosures of that data?

---

[18] NCVHS Report to HHS, (June 22, 2006)

[19] Ethical Principles for Medical Research Involving Human Subjects, World Medical Association Declaration of Helsinki, June 1964

[20] NCVHS Report to HHS, (June 22, 2006)

[21] Ethical Principles for Medical Research Involving Human Subjects, World Medical Association Declaration of Helsinki, June 1964

[22] The Texas Tribune, TribBlog, Lawsuit Alleges DSHS Sold Baby DNA Samples, Becca Aaronson, December 8, 2010 at: http://www.texastribune.org/texas-state-agencies/department-of-state-health-services/lawsuit-alleges-dshs-sold-baby-dna-samples/

[23] New York Times, Indian Tribe Wins Fight to Limit Research if Its DNA, Amy Harmon, April 20, 2010 at: http://www.nytimes.com/2010/04/22/us/22dna.html?ref=us

[24] Healthcare it News, Kaiser genomics project completes first phase, Molly Merrill, Associate Editor, July 25, 2011 at: http://www.healthcareitnews.com/news/kaiser-genomics-project-completes-first-phase

Absent informed consent for the use and disclosure of PHI for research, robust AODs and access reports are essential so the public can know when and what diseases and conditions are being studied by researchers and public health authorities.

Researchers argue that they must have access to entire populations for some kinds of research. That has never been possible; researchers have always had to extrapolate to provide good enough answers to research queries. The choice is between having less data than some researchers want to have and driving significant numbers of patients away from treatment because they will know there is no other way to protect their privacy. When patients learn that they can trust HIT systems, data exchanges, and researchers, they will provide MORE data and MORE accurate data because they trust that it will not be used or sold to harm them. Counter-intuitively, privacy (patient consent and control over data for routine uses and all research uses) will improve data quality, accuracy, and integrity. The most chilling effect in research will come not from requirements for human subject research as stated on page 31432, but from eliminating the foundational ethical principle of obtaining informed consent for research. Why do that when technologies can make finding potential research subjects cheap and easy with consent.[25]

Finally, the burdens on researchers to provide AODs are no more difficult than for any other users of HIT and PHI. Thanks to the required HIPAA and HTECH data security requirements, the minor additions so users can add a "purpose" for the use or disclosure and adding technology to automatically allow patients to download AODs means researchers will have minimal burdens.

Consent in Future HIT Systems and Data Exchanges, the Need for a Patient-Centric Vision based the Law and Medical Ethics

HHS does not appear to envision a future where patients will easily be able to electronically set up and change consent directives in one place for broad categories of data use, for any narrow specific uses and disclosures of PHI, and for any specific or broad exclusions of access or disclosure to selected people or entities to data for treatment, payment, and/or healthcare operations. HHS does not appear to support the use of technology to improve consent or control over PHI. Instead, stimulus funds are being invested in technologies that violate the public's rights and expectations to control the use of PHI for routine uses, research, and public health (unless required by law).

Trustworthy HIT systems and data exchanges should enable patients to easily exercise their longstanding rights to health information privacy and control over PHI in one place, rather than being forced to set consents everywhere their data exists, which there is no way of knowing

[25] Private Access consent technologies were developed to aid researchers looking for appropriate subjects quickly and easily using electronic tools for informed consent. See "live" demonstration at the Consumer Choices Technology Hearing in 2010 at: http://nmr.rampard.com/hit/20100629/default.html

today. In the future, all holders of PHI should check electronically with patient consent directives before using or disclosing PHI, similar to the way that pharmacies electronically and instantly check with PBMs to determine patient co-pays and drug formularies. With consents in one place, as patients' preferences change they can instantly change their directives.

Robust consent management and segmentation technologies exist and have clearly worked well for over 9 years[26], and since we also know that technology can enable patients to easily and cheaply be contacted for consent to use or disclose PHI by cell phones and computers, there is no longer a reason to use IRBs or Privacy Boards to approve the use of PHI for research, quality improvement, comparative effectiveness research, population health, etc, etc. Patients can give informed electronic consent for research use of their PHI.

Dr. Don Berwick, head of CMS, envisions a future patient-centered health care system where "Medical records would belong to patients. Clinicians, rather than patients, would need to have permission to gain access to them." [27] My proposed definition of "patient-centered care" is this: The experience (to the extent the informed, individual patient desires it) of transparency, individualization, recognition, respect, dignity, and choice in all matters, without exception, related to one's person, circumstances, and relationships in health care . . ."

Further he wrote, "I freely admit to extremism in my opinion of what patient-centered care ought to mean. I find the extremism in a specific location: my own heart. I fear to become a patient. . . . What chills my bones is indignity. It is the loss of influence on what happens to me. . . . That's what scares me: to be made helpless before my time . . . to be alone when I need to hold my wife's hand, to eat what I do not wish to eat . . . to be told when I wish to be asked… Call it patient-centeredness, but, I suggest, this is the core: it is that property of care that welcomes me to assert my humanity and my individuality. If we be healers, then I suggest that that is not a route to the point; it is the point."

Patients' Legal and Ethical Rights[28] to Control Health Information

"Congress has previously found that Americans have a right to privacy for personal information about themselves that is a "personal and fundamental right protected by the Constitution of the United States".[29] The federal courts and the Department of Health and Human Services have recognized that the right to privacy has two branches. One branch is "the individual interest in avoiding disclosure of personal matters" (informational privacy) and the other is "the interest in

---

[26] Ibid. See videos of consent and segmentation systems in use over 10 years for 4 million patients demonstrated "live".

[27] Health Affairs 28, no. 4, 2009: What 'Patient-Centered' Should Mean: Confessions Of An Extremist: A seasoned clinician and expert fears the loss of his humanity if he should become a patient, Donald M. Berwick, see: http://patientprivacyrights.org/wp-content/uploads/2010/02/What-Patient-Centered-Should-Mean.pdf

[28] Excerpted from The Right to Health Information Privacy, James C. Pyles, July 10, 2008

[29] Pub. L. 93-579, section 2(a)(4).

independence in making certain kinds of important decisions" (decisional privacy).[30] HHS has stated that the interest in informational privacy is the interest addressed by HIPAA Privacy Rule.[31]

Prevailing federal case law provides that "[t]here can be no question that an [individual's] medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection…[defined as]…control over the knowledge about oneself."[32] The right to informational privacy is "one of the most cherished rights of American citizenship commonly characterized as "the right to be let alone".[33] Medical records and information stand on a different plane than other relevant materials" and are generally afforded a higher level of privacy protection.[34] If there is no right to privacy for one's health information, which may include information on a person's genetic make-up and inner-most thoughts, a right to privacy might not exist for any information.

Federal courts have found that the constitutionally protected right to highly personal information, including health information, has become so well established that no reasonable government employee could be unaware of it.[35] Further, the courts have noted that "[t]he right not to have intimate facts concerning one's life disclosed without one's consent…is a venerable one whose constitutional significance we have recognized…".[36]

The right to privacy of personal information, including health information, is recognized under the tort law or statutory law of all 50 states, and 10 states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington) include a specific right to privacy in their state constitutions.

In addition, the right to not have one's health information disclosed without one's consent is a core concept of both the Hippocratic Oath and the ethical standards of "virtually all health professions".[37] The American Medical Association (AMA) recently re-affirmed this ethical policy in the context of electronic health information systems:

- "Our AMA policy is that where possible, informed consent should be obtained before personally identifiable health information is used for any purpose."[38]

The ethical principles of other professional associations similarly provide:

---

[30] Whalen v. Roe, 97 S. Ct. 869, 876 (1977). 65 Fed. Reg. at 82,464 (Dec. 2000).
[31] 65 Fed. Reg. at 82,464.
[32] United States v. Westinghouse, 638 F.2d 570, 577, n. 5 (3rd Cir.1980).
[33] United States v. Westinghouse, 638 F.2d at 576.
[34] United States v. Westinghouse, 638 F. 2d at 577.
[35] Gruenke v. Seip, 225 F.3d 290, 302-03 (3rd Cir. 2000); Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).
[36] Sterling v. Borough of Minersville, 232 F.3d at 195.
[37] Finding of the National Committee on Vital and Health Statistics, report to HHS, p. 3 (June 22, 2006).
[38] American Medical Association, Report 19 of the Board of Trustees (A-07), Patient Information in the Electronic Medical Record.

- "Confidentiality of the patient's communications is a basic patient's right and an essential condition for effective psychoanalytic treatment and research. A psychoanalyst must take all measures necessary to not reveal present or former patient confidences without permission, nor discuss the particularities observed or inferred about patients outside consultative, educational or scientific contexts."[39]

Finally, the U.S. Supreme Court has found based on the "reason and experience" of the country, that communications between a patient and a psychotherapist, are subject to a "psychotherapist-patient privilege" which can only be waived by the patient.[40] The psychotherapist-patient privilege recognized at the federal level has also been recognized by all 50 states and the District of Columbia. The Supreme Court has noted that this privilege serves both the interest of the individual and the public in permitting access to effective psychotherapy and that unless such a privilege were recognized, communications essential for effective psychotherapy would simply not occur.

So, the right to privacy and security for health information is well established, and nothing … is intended to alter or diminish that right in any way."

HHS' decisions in this NPRM do not fit with the existing legal and ethical rights specified in Pyles' paper on "The Right to Health Information Privacy" or in federal laws known as 42 CFR Part 2 or "7332" for the privacy and confidentiality of disclosures of military health records and in addition violate Congress' intent that patients have the right to robust accounting of disclosures of PHI from electronic systems.

Industry Objections to Robust, Detailed Accounting of Disclosures Required by HITECH

Industry complaints about the burdens, costs, and time needed to implement the consumer protections intended by Congress seem grossly exaggerated. As HHS repeatedly pointed out in the NPRM, existing HIPAA Security requirements that specify CEs and BAs must monitor/audit access and disclosures of PHI have been in place for some time, and provide most of the data required for AODs.

Creating a full, detailed AOD with exact dates and names need not be a difficult manual process as stated (page 31429 of the NPRM), but can easily be accomplished technically with a minor add-on so users can specify the purpose of the access, use or disclosure. Robust authentication system logs required for data security provide all the other information HITECH specifies AODs to provide. Much like the VHA's "Blue Button" for downloading PHI from EHRs, AODs could be automated so that patients could download them at any time. Cost and burdens to CEs and BAs

[39] The American Psychoanalytic Association, Principles and Standards of Ethics for Psychoanalysts, Guiding General Principles, IV. Confidentiality.
[40] Jaffee v. Redmond, 116 S. Ct. 1923 (1996).

would then be the minimal costs of designing technology to permit patients to obtain AODs themselves.

Obviously HIT upgrades take time and there is always some cost associated with upgrades, but these costs for accounting of disclosures should be minimal. In fact, many proprietary HIT companies sell or are building new products that offer detailed accounting of disclosures. There is no reason NOT to require robust accounting of disclosures right away, because the information from the process of authenticating user access to EHR systems collects most of the needed data already. It would not be hard to tweak the authentication process to add another data field so users can fill in a detailed purpose/description of the use or disclosure.

Imprivata offers one example of a robust accounting of disclosure system (there are many other authentication technology firms that offer similar products):

Imprivata's PrivacyAlert™ Detects Snooping and Identity Theft[41]

- detects snooping, identity theft and inappropriate access
- automated and scalable privacy monitoring
- investigate and report data breaches
- investigate employees, patients or both
- Out-of-the-box supports all leading healthcare applications---Eclipsys, GE Centricity Enterprise, MEDITECH Magic, Siemens Invision, etc

The request for years of delay before implementing robust AODs makes no sense, given existing requirements to have technologies to monitor security and audit access to and disclosures of PHI.

AOD data should be retained the length of time specified in HITECH. Congress intended six years, not three, for data retention. The breach remediation industry reports that it can take a minimum of two years for a victim to discover medical identity theft. Therefore three years is clearly not enough time to retain data to trace the source of medical identity theft, a growing and very expensive way people are harmed. It can also take years to discover other harms from inappropriate use, access, disclosures, or data sales of PHI. As we learned from the recent massive scandal at the UK's News of the World, proving who hacked into and misused sensitive cell phone data would have been impossible if records were only retained three years.

Automating the process of collecting and reporting AODs to patients or enabling patients to download AODs themselves will have minimal costs to CEs or BAs. Patients should not be charged. No one should have to submit requests for AODs in writing; technology should be used to improve consents.

---

[41] See: http://www.marketwire.com/press-release/Imprivatas-New-Product-Helps-Hospitals-Proactively-Investigate-Audit-Access-Patient-1123908.htm

We agree that "access reports" will be very valuable for patients, and need not have all the detail required for AODs. However, the kind of robust, detailed AODs Congress specified in HITECH are a far more valuable consumer protection and right. HHS should not violate that right by implementing regulations that weaken the AODs. The requirement to include which information was accessed is very important to consumers. Every detail Congress specified matters to consumers and can be collected automatically with minor technology add-ons. We agree that all access and disclosure should be reported in the "access reports" because individuals want the most complete picture of who has seen or used their PHI. Consumers should be able to get AODs from insurers, pharmacies, labs, clearinghouses, and x-ray facilities. All CEs and BAs should be required to provide the all details about the uses and disclosure of PHI Congress intended to be part of AODs. People really DO want to know the details, descriptions, and purposes of all internal and external access and disclosures of PHI. It is critical for consumers to be able to learn which entities and providers use and disclose their PHI in accord with their rights and expectations.

The assumption that few patients will want detailed AODs is unlikely. People will be as interested as they were in obtaining copies of their medical records via the VHA "blue button". They really want to learn what happens to their PHI and who sees it.

Providing machine readable formats is not a burden since most of that work was accomplished in order to be able to monitor and audit health data security by looking at all access and disclosures of PHI.

There is no evidence cited in the proposed rule that Congress intended to narrow the scope of information to which the right to an accounting of disclosures would apply.

Conclusion

In HITECH, Congress very deliberately eliminated the prior HIPAA exception to AODs for TPO because most uses and disclosures of PHI occur for routine purposes that fall under TPO. Congress wanted individuals to be able to tell if their health information was being used or disclosed lawfully. In short, without detailed information in AODs for TPO, individuals literally have no way to know where their PHI goes or who sees it and can only trust that CEs and BAs do not improperly use and disclose their personal health information. We can't trust unless we can verify. AODs provide consumers with the essential information need to verify. We respectfully urge HHS to rework the NPRM to comply with HITECH, not violate it.

Sincerely,

Deborah C. Peel, MD

Founder and Chair, **Patient Privacy Rights**
O: (512) 732-0033

www.patientprivacyrights.org