NYUSteinhardt
Steinhardt School of Culture, Education, and Human Development

**DEPARTMENT OF MEDIA, CULTURE, AND COMMUNICATION**

*Helen Nissenbaum, Professor*
*http://www.nyu.edu/projects/nissenbaum*

December 9, 2011

Joy Pritts, JD
Chief Privacy Officer
Office of the National Coordinator for Health Information Technology
US Department of Health & Human Services
202-690-3955 (tel)

Dear Joy Pritts:

We are pleased to offer remarks on the recent HHS Notice of Proposed Rulemaking covering changes to Accountings of Disclosure from the perspective of active privacy research. As members of the SHARP Security (http://www.SHARPS.org) research project, we recognize that decisions relatively early on in the design and regulation of health information systems can have implications not only for the utility of these systems but their compatibility with the public interest and values.

Please do not hesitate to contact us if you have questions or would like further clarification.

Sincerely,
Joseph Lorenzo Hall,
Postdoctoral Research Fellow, SHARPS Project
Helen Nissenbaum, Co-PI, SHARPS Project

239 Greene Street, 7th Floor | New York, New York 10003
212 998 5251 phone | 212 995 4046 fax

**December 9, 2011**

**To:** **Joy Pritts, JD. Chief Privacy Officer**
**ONC for Health Information Technology**
**From:** **Helen Nissenbaum (Co-PI) and Joe Lorenzo Hall (Postdoctoral Fellow)**
**SHARP Security Project (http://www.sharps.org)**
**Subj:** **Analysis and Recommendations concerning HHS Notice of Proposed Rulemaking covering changes to Accountings of Disclosure**

## Introduction

This view of the recent notice of proposed rulemaking (NPRM) concerning accountings of disclosure (AOD) of personal health information (PHI) under the HITECH Act[1] is offered from the perspective of privacy researchers, currently funded by The Department of Health and Human Services (HHS) under the SHARPS grant.[2] To prepare, we read a representative selection of the comments submitted to HHS in order to canvass issues and interests implicated by the NPRM. Starting with a random selection of approximately 30% (132) of the 435 comments posted at regulations.gov,[3] we browsed the remaining entries in the docket and selectively read additional comments that we thought might express distinctive perspectives—from advocates, covered entities (CEs), business associates (BAs), vendors, service providers, academics, trade groups and members of the public.[4]

In what follows we: (1) briefly summarize findings from this sample of public comments; (2) highlight and evaluate three prevalent clusters of concern; (3) present a framework for evaluating the proposed accounting of disclosure and access report based on the *theory of contextual integrity*; and, (4) offer our own

---

[1] *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* 76 Fed. Reg. 31426-31449 (May 31, 2011; RIN 0991–AB62). (AOD NPRM)

[2] *See:* http://sharps.org/

[3] In addition to the many unique comments received in response to the NPRM, we noted at least two types of form-letter comments from hospitals and emergency medical service (EMS) providers that were submitted many times by different organizations. For examples, see: Kansas Hospital Association, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (July 29, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0157; and, West Shore EMS, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0254.

[4] We cite specific comments in the discussion below. The list of these specifically-chosen comments includes comments by: The Medical Group Management Association, World Privacy Forum, IMS Health, AIDS Healthcare Foundation, Consortium of Independent Review Boards, Stanford University's School of Medicine, Hospitals and Clinics, Intermountain Health Care, Patient Privacy Rights, Planned Parenthood Federation of America, Center for Democracy in Technology, Epic, Privacy Rights Clearinghouse, Fidelity Investments, Kaiser Permanente, the American Medical Association, a number of individual comments from physicians and patients and one anonymous submission from a medical transcription company (*see:* http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0214 ).

recommendations for setting up accountings of disclosure and shaping access reports, including recommendations for new research.

## 1. General Findings

The comments are highly polarized, but even among those opposed to the AOD NPRM, we noticed several distinct perspectives. Among them, industry and privacy advocates provided the most substantively engaging comments.

A recognizable group of commenters, including many in the health care industry, argued that the proposed rule is overly burdensome, ineffective and, in some cases, dangerous. These commenters, on the one hand, welcomed proposed modifications to the AOD that would reduce the burdens on CEs by clarifying what disclosures are covered, and shortening the length of time CEs and BAs need to keep disclosure records, but on the other hand, strongly opposed the introduction of a right to an access report. They argue that HHS had over-stepped its regulatory authority by requiring reporting for any access to PHI in an "electronic designated record set" (eDRS)—rather than an electronic health record (EHR) as specified in the text of the HITECH Act.[5] Further, they suggested that because HHS does not understand the variety of isolated systems in which PHI in an eDRS exists, its estimate of the burden on CEs in implementing and providing an access report is erroneously low.

A second group of commenters, fewer and not as unified in substance, consist of privacy advocates. Privacy advocates argue largely the opposite: both that the rule goes too far in exemptions and that it will not be burdensome for CEs to provide the proposed AODs/access reports. A number of advocates protest that excluding certain types of PHI disclosures from AODs will make them less useful; AODs will not be comprehensive dossiers that give a patient a detailed view on how their PHI is disclosed, but instead will have gaping holes where certain types of disclosures are missing.[6] Advocates, with some exceptions,[7] comment that access logs will not be difficult to produce and should be translated into an easily digestible format for patients.

Some individuals who did not draft formal comments chose instead to include a brief comment directly through the regulations.gov site. These tended to be

---

[5] § 13405(c)(1)(A) of HITECH removes the exemption from the Privacy Rule for disclosures of made for treatment, payment and healthcare operations by saying such exemption "shall not apply to disclosures through an electronic health record", but it does not use the "electronic designated record set" language of the AOD NPRM. *See:* The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5).

[6] For example, the World Privacy Forum comments that the changes in exemptions from disclosure offer "the appearance of Swiss cheese, a seemingly solid mass with numerous unpredictable holes of varying dimensions". *See:* World Privacy Forum, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0297 at 7.

[7] E.g., the comment from the Center for Democracy and Technology accepts that they were earlier overly optimistic about the technical capabilities of health information systems with respect to access logging. Center for Democracy And Technology, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0288 at 3.

informal but enlightening, registering concerns of individual patients or physicians, outside of an organizational context. For example, some physicians reported on potential burdens this kind of rule might impose on their practices and patients reported on past adverse medical privacy events.

## 2. Clusters of Concern from the AOD NPRM Comments

Because the scope of this note does not allow for a thorough review of comments, we are focusing on three important themes around which many of them clustered: (1) Patients currently do not request AODs and therefore there is no obvious use for AODs and access reports; (2) Patients will not understand AODs and access reports when they are provided; and; (3) The burden required to produce access reports is excessive.

### 2.1. Low Usage Rates for the Right to Accounting of Disclosures

In the preamble to the NPRM, HHS pointed to low numbers of patients requesting AODs. Many CE and BA commenters reinforced this with estimates ranging from zero[8] to an average of 7 per month per facility.[9] The Medical Group Management Association surveyed its members and reported that approximately half receive no requests for AODs per physician per year and only 6% receive 10 or more such requests.[10] Clearly, only a limited subset of patients knows about and exercises the right to an accounting of disclosures of PHI granted to them under the HIPAA Privacy Rule.

Many commenters found fault with the logic HHS used to justify the access report based on historically low request rates arguing that if few people request an access report, CEs will not have to expend much effort to produce them.[11] In claiming so, commenters said, HHS overlooks the fact that the bulk of costs to CEs will not be the marginal costs of producing successive access reports (as is the case now with AODs) but the sunk costs of integrating systems necessary to produce an aggregated access report, no matter how few. Many CE commenters, such as the trade group MGMA, used low usage statistics to counsel *against* new rights to an access report, arguing that the benefit to patients does not outweigh the burdens to CEs.[12] A notable exception from the industry perspective is the comment from the North Carolina Healthcare Information and Communications Alliance (NCHICA), which argued largely the same but went further to point out that patients' increasing concerns about unauthorized access to PHI would likely

---

[8] Tillamook County General Hospital, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0434 at 2.

[9] Kaiser Permanente, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0356 at 12.

[10] Medical Group Management Association, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011) at 14-15, available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0374 at 6.

[11] 76 Fed. Reg. 31439.

[12] MGMA Comment, note 10, at 5-6.

increase interest in access logs.[13] Advocates such as the World Privacy Forum (WPF) and Patient Privacy Rights made a particularly strong case for future increases in requests for AODs and access reports.[14] As these requests become as routine as requests for electronic medical information itself, obtaining such reports should be made as easy as the Veteran Health Administration's "Blue Button" tool for downloading health information.[15]

Ultimately, the intent behind providing patients with information about PHI disclosures is to promote accountability and transparency. It is reasonable to expect that as requests for health records increase, interest in how those records are accessed and used is likely to increase as well. Designing AODs as an effective vehicle for promoting transparency and accountability in PHI disclosure can help to alleviate patients' growing concerns about privacy[16] in their health information. Historical usage statistics are one measure of value for the existing AOD but do not help to evaluate whether or not it effectively promotes these interests. Research measuring awareness of the AOD right and the extent to which the AOD supports learning about disclosures of PHI is essential in deciding how to structure modified rights to disclosure accounting.

### 2.2. Patient Understanding of AODs and Access Reports

Observing that patients are already overwhelmed by the amount of information in an AOD, CE and BA commenters largely argued that this would only get worse with the access report. Access reports will document each *access* of PHI in electronic form, not just disclosures of PHI, so they will be quite voluminous, amounting to hundreds of pages for a typical hospital stay.[17] In fact, a number of years ago, Kaiser Permanente instituted a program offering patients EHR access logs, but discontinued it after finding little benefit to patients.[18] The proposed access report may be similarly unusable and incomprehensible to patients if it reports potentially each and every access to PHI. Patients need a more usable form of less-comprehensive information.

The answer to commenters who suggest that low usage is likely due to patients' ignorance of the right to AODs and lack of utility of such information is for CEs and vendors to modify them and create reports that patients *will* find useful and usable. The field of, "user-centered design" (UCD), an analog to privacy by design (discussed below in Section 2.3), seeks to promote usability of software and

---

[13] North Carolina Healthcare Information and Communications Alliance, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (July 28, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0140 at 4-5.

[14] WPF Comment, note 6 at 2-3.

[15] Patient Privacy Rights, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 2, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0417 at 12-13.

[16] "Americans' Opinions about Healthcare Privacy", Ponemon Institute, (February 2010), available at: http://www.ponemon.org/local/upload/fckjail/generalcontent/16/file/Americans'%20Opinions%20about%20Healthcare%20Privacy%20Final%202.pdf at 1.

[17] Fairview Health Services, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0412 at 7.

[18] Kaiser Comment, note 9, at 4.

output—such as AODs, access reports and tools meant to help interpret them—during product design and development. Testing design ideas with mock-ups and prototypes on potential users during the design stages of product development is aimed at producing more useful and usable results.[19] It is unclear to what extent CEs and vendors have employed UCD processes, especially since disclosure accounting features are not major selling points of their products. Because engaging patient-users with AODs is a crucial element of honoring the intent of the Privacy Rule, HHS might consider specifying regulations for more useful accounting mechanisms, better able to support disclosure accountability and transparency.

### 2.3. Burden of Providing Access Reports

Many CEs commented that modifications to support the access report are excessively burdensome and would need to be developed within an existing environment of intense information system changes. For example, NCHICA estimated 10,000 hours of development time, on top of current efforts to meet other time-sensitive mandates, such as the Stage-1 Meaningful Use criteria and the ICD-10 classification system.[20] The Blue Cross Blue Shield Association (BCBSA) estimated the total cost of modifying their systems to support access reports across their 39 independent BCBSA health plans would be $1.5 Billion.[21] In fact, of the industry comments we reviewed, only one, from FairWarning, Inc., claimed that producing an access report as outlined in the NPRM would be "technically feasible and affordable"[22]—and FairWarning has a direct economic stake.[23] Clearly, HHS misjudged the ease of implementation of the access report.

This poses a conundrum: The burden of complying with the access report requirement, on top of other ongoing compliance efforts could result in projects falling short on both the added requirements as well as the original ones. The proper course of action, however, is not necessarily to abandon the access report

---

[19] Rubin, J., and D. Chisnell. *Handbook of Usability Testing: how to plan, design, and conduct effective tests*. Wiley, 2008.

[20] NCHICA Comment, note 13, at 7.

[21] Blue Cross Blue Shield Association, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0362 at 1.

[22] FairWarning, Inc., Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (July 27, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0113.

[23] Two commenters, the Association of American Medical Colleges and University Hospital Augusta, reported that implementing FairWarning's software across their entire system would be exceedingly expensive, amounting to $17-18,000/year per application, with about 100 hours of staff time per application. For University Hospital Augusta doing this for all 102 of their applications would cost $1.3 million/year and four to six additional staff. *See:* Association of American Medical Colleges, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0283 at 4; University Hospital Augusta, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (July 27, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0430 at 4.

requirements, but instead to increase the amount of time given to CEs to complete them all.[24]

We do not favor allowing CEs and vendors delay consideration of features that support disclosure accounting because past experience suggests that employing a privacy-conscious design process, not adding privacy on at the end, yields superior results. "Privacy by design" has gained increasing support as an approach to developing privacy-enhancing and privacy-protective technologies.[25] The Federal Trade Commission as well as the Department of Commerce have both endorsed it in recent whitepapers,[26] while the International Conference of Data Protection and Privacy Commissioners adopted a resolution recognizing it as an essential component of protecting privacy.[27]

Comments lamenting further modifications to systems during this time of change miss the point that privacy is not something to "bolt on" after current development is completed but affirmatively factored in at the outset, as with properties such as availability, reliability and interoperability. While leaving plenty of room for variation in HIT design, HHS should be able to recommend privacy by design as a crucial element of privacy protection and insist that AODs, access reports and other elements of health privacy not be wrappers added on afterwards. In providing substantive guidance on how HIT systems ought to better support disclosure accounting now, HHS might be able to avoid problems where industry interpretations of older rules may conflict with HHS' current interpretation.[28]

## 3. A Framework for AOD from Contextual Integrity

The concerns discussed above might seem to pose an impossible conundrum with harsh trade offs as the only solution. Contextual integrity, however, unravels

---

[24] The HITECH Act permits postponement of the new AOD requirements to 2016. *See:* § 13405(c)(4)(C) of HITECH, note 5.

[25] Ann Cavoukian, *Privacy By Design… Take the Challenge*. Information and Privacy Commissioner of Ontario, Canada, 2009, available at: http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf .

[26] "Staff Report. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers", Federal Trade Commission, (December 2010), available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf ; Internet Policy Task Force, "Commercial Data Privacy and Innovation in The Internet Economy: A Dynamic Policy Framework", Department of Commerce, (December 2010), available at: http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf .

[27] "Privacy by Design Resolution", International Conference of Data Protection and Privacy Commissioners, (27-29 October 2010), Jerusalem, Israel, available at: http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf .

[28] For example, in the AOD NPRM narrative, HHS cites the fact that under the HIPAA Security Rule CEs must already have the capability to log PHI access and should be able to easily produce the access report for which the AOD NPRM calls. (*See:* AOD NPRM, note 1, 76 Fed. Reg. at 31429.) However, many commenters disputed this interpretation. For example, the Medical Group Management Association (MGMA) argued that the Security Rule does not say that these systems must necessarily record access in manner and nature that HHS specifies for the access report, but that CEs must make reasonable and appropriate audit methods given the organization's own risk analysis and organizational factors and the capabilities of organizational information systems. (*See:* MGMA Comment note 10, at 14-15.) This indicates that CEs could meet the requirements of the Security Rule by using audit methods that do not consist of recording audit logs with the elements HHS envisions for the AOD NPRM's access reports provision.

some of the apparent contradictions among privacy, excessive burden, and incomprehensibility and suggests a way forward that addresses them all in some measure.[29]

As a theory of informational privacy, contextual integrity views the heart of our concern to be appropriate flows of personal information, and not, as do other accounts, as concerns over control or secrecy. Appropriateness is determined according to social **context: actors** (*senders* and *recipients* sharing information about *subjects*) communicating **types of information** under **principles of transmission** (constraints on information sharing). These elements define an "information flow" and context-specific **informational norms** are posited as rules prescribing information flows that are appropriate in given circumstances. Flows that do not respect entrenched informational flows violate contextual integrity and may constitute violations of privacy, depending on the effects novel flows have on general moral and political values as well as on the achievement of ends, purposes, and values of the context in question. In healthcare, the latter would include, in general terms, effective medical care, lower healthcare costs and positive health outcomes.

For a start, contextual integrity provides a framework for expressing the exceedingly complex information flows among healthcare providers, business associates and other entities.[30] It also hypothesizes that people will be particularly attuned to and concerned about flows of information that violate expectations, are inappropriate, or not conducive to the delivery of efficient and high-quality health care, improving health, and so forth. For example, sharing medical information about a patient with a specialist—an expert consulted in the course of treatment—is an information flow that patients will expect and likely not find troubling. However, sharing PHI with a data aggregator for marketing purposes might be jarring even if a patient has given nominal consent by signing off on a provider's privacy policy giving notice of this practice. In between, there are flows of information that patients are not generally aware of, but must exist for the larger health care system and public health mission to function. For example, reporting detailed, historical PHI to a patient's insurance provider may seem excessive to patients who might believe that a report on their current problems and medical procedures are sufficient for billing purposes. Similarly, reporting detailed PHI to government health surveillance organizations may seem unnecessary to patients, who may not understand the importance of monitoring medical incidents in order to protect the aggregate health of a society.

---

[29] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford University Press, 2010

[30] For a visualization of health information flows in 1997, immediately after HIPAA's passage, see figure 3.1 on p. 73 of: Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *For the Record: Protecting Electronic Health Information* (1997), http://www.nap.edu/catalog.php?record_id=5595. For a set of figures that compares the flows of health information from 1997 to 2010, after HIPAA's Privacy Rule had been in effect for a number of years, see figures 1 and 2 of: Latanya Sweeney, Public Comment on *Advanced Notice of Proposed Rulemaking: Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators*, (2011), available at: http://dataprivacylab.org/projects/irb/DataPrivacyLab.pdf.

Contextual integrity can guide decision making to distinguish disclosures that can be excluded from AODs, namely, those that are routinely expected, from those that should be included because they are unexpected, for example, those involving researchers, marketers and public health oversight authorities, and, of course, breach notification disclosures.

It might be useful to elaborate the approach by demonstrating the application of contextual integrity to specific AOD exemptions in the NPRM:

- **Breach Notification:** Contextual integrity would weigh against exempting disclosures for which a covered entity has provided breach notification.[31] Impermissible disclosure through a breach is, by definition, an inappropriate flow of protected health information. As such, it is precisely something patients would want highlighted in an AOD and/or access report. As many privacy advocates noted, providing a breach notification does not necessarily mean that individuals would receive such a notice.[32] The AOD report should aim to provide notice of both permissible and impermissible disclosures of interest to patients in one reasonably comprehensive document. Further, since the detail required in a breach notification is much less than the per item requirement in an AOD, it would not constitute an additional burden on covered entities.
- **Child/Adult Abuse and Neglect; Domestic Violence:** Contextual integrity would generally concur with the NPRM proposal to exempt reports of child abuse and neglect and adult abuse, neglect and domestic violence from AODs.[33] Because any flow of such information back to parents, spouses or guardians might result in further harm to patients or members of the healthcare workforce this exception to normal flows is defensible. In fact, some commenters have urged widening its scope to include cases in which patients or healthcare workers might be at risk of harm, for example, from mental patients or patients with criminal histories or histories of violence.[34] Accordingly, a more generic exemption, as proposed by Planned Parenthood Foundation of America in its comment[35]—to exempt disclosures that might significantly harm either the patient or a healthcare worker—has merit.
- **Research Disclosures:** By the measure of contextual integrity, allowing exemptions from disclosures for research, where an institutional review board (IRB) has waived the requirement for patient authorization after determining minimal risk to the patient,[36] ought to rest on several factors. Based on a letter from Secretary's Advisory Committee for Human

[31] 76 Fed. Reg. 31431.
[32] WPF Comment, note 6, at 9; CDT Comment, note 7, at 11; Privacy Rights Clearinghouse, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0405 at 4–5.
[33] 76 Fed. Reg. 31431-31432.
[34] While a number of commenters spoke to this concern, see, generally: Planned Parenthood Foundation of America, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (August 1, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0372.
[35] PPFA Comment, note 34, at 4.
[36] 76 Fed. Reg. 31432–31433.

Research Protections (SACHRP) and an Institute of Medicine (IOM) report the rationale for the exemption is to alleviate the heavy burden placed on research-active institutions at little cost to privacy. Factors relevant to whether an exemption is warranted include how sound is the assessment of minimal risk and how solid are the assurances of state-of-art data practices, for example, anonymization. Learning how patients might react to the news that their records are utilized in these ways is essential to ensuring trust is sustained among patients, caregivers, and researchers, all potentially harmed if a breakdown were to occur. Such questions might be approached in a variety of ways and utilizing a variety of methods. (Also relevant to these explorations is the point noted by researchers that keeping track of granular accesses to PHI could actually increase the risk to human subjects.[37]) Here, we suggest continuing the protocol listing currently required by the AOD rules but reduce the burden on CEs by eliminating the requirement that they assist patients in contacting researchers. We further suggest more research is needed as to the interest of patients in learning about research-related PHI disclosures.

- **Health Oversight Activities:** The NPRM proposed exemption for health oversight activities required by law[38] is most likely compatible with contextual integrity. As long as oversight agencies to whom CEs are disclosing PHI are following best practices in their handling of information and using it only for administrative purposes and to ensure quality of care and accountability, there seems to be no cause of concern for patients.
- **Otherwise Required By Law:** For contextual integrity, a blanket exemption for disclosures required by law,[39] apparently mostly state laws, is problematic. Although there might be reasons for exempting certain disclosures, for example, as might be required for law enforcement or public health, one would need to treat these disclosures on a case by case basis, in each case assessing the impacts on patients, other actors, and the values, ends, and purposes of the healthcare context. Learning about these disclosures may potentially serve a useful educative purpose for patients, particularly when they move from one state to another and in so doing are made aware of different requirements in respective states.

## 4. Recommendations

- Research is needed to explain the documented low incidence of exercising the current right to an AOD to guide practices going forward.
- Access reports must be relevant and meaningful to patients while not excessively and unreasonably burdening CEs.

---

[37] Massachusetts General Hospital researchers commented that this will increase risk to patients whereas no linked identifier would have been used before such a rule, a linked identifier would now have to be used to log researcher accesses to PHI and be able to subsequently report those back to the patient. *See:* Massachusetts General Hospital, Public Comment on *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act,* (July 26, 2011), available at: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0107 at 2–3.

[38] 76 Fed. Reg. 31433.

[39] 76 Fed. Reg. 31433.

- Contextual integrity focuses attention on disclosures that are likely to be important to patients thereby important to include in AODs and access reports.
- Human factors research is needed to enable patients to understand and navigate around AODs and access reports. Such findings should inform the design of instruments, apply state-of-art visualization techniques for data and metadata, and anticipate answers patients are likely to be seeking,
- A reasonable timeline should be determined in order for analytical and empirical research findings to inform product design. Designers, builders, and vendors of access report systems should be discouraged from taking these findings into consideration only as an afterthought and instead do so "by design."

## 5. Conclusion

AODs are crucial vehicles for transparency and accountability with respect to the HIPAA Privacy Rule. By focusing attention on disclosures that are meaningful rather than merely complete, the framework of contextual integrity can help to define effective artifacts that are not unnecessarily burdensome for CEs. HHS, too, has a role to play in defining a substantive vision of the shape and content of AODs and access reports, encouraging privacy by design and user-centered design, and determining a reasonable timeline for compliance.