Accountings of Relationships

Joseph Lorenzo Hall[1], Benedicte Callan[2], Helen Nissenbaum[1]

[1]Department of Media, Culture & Communication, New York University
[2] Lyndon B. Johnson School of Public Affairs, University of Texas at Austin

1 Introduction

In 2011, the US Department of Health and Human Services (HHS) issued a proposed rule [1] that would amend the HIPAA Privacy Rule to require covered entities to provide audit logs to patients upon request. This would allow patients to know how their personal health information (PHI) is being disclosed. The focus on patient-centered reporting of access to PHI comes from the Privacy Rule's structure which is grounded in fair information practices (FIPs), a set of best practices revised over decades [4]. In terms of disclosure of personal information, a key principle from FIPs includes, "There must be a way for an individual to find out what information about him is in a record and *how it is used*." (emphasis added)

The current mechanism in the Privacy Rule to support this principle is called an accounting of disclosure (AOD). An AOD provides to a patient upon request a detailed listing of past disclosures of PHI — i.e., sharing PHI outside of the organizational boundary — by their provider, whether the disclosure was made in paper or electronic form, over a six-year period.

The proposed rule would modify AODs and introduce the idea of an "access report" (AR). An AR would be required to cover any accesses made to electronic PHI over the past three years. Instead of reporting on *disclosures* of PHI outside of the organizational boundary, ARs would report each time electronic PHI was *accessed*, whether internally by an employee or as an extraorganizational disclosure. ARs are "fine-grained AODs" that tell a patient who accessed their PHI and when the access was made.

2 Problems with AODs and ARs

The comments submitted in response to the proposed rule were largely negative, arguing that the AR, in particular, would be burdensome, ineffective and even dangerous in some cases [5]. Burdensome, in that the scope of material covered by AODs/ARs changed dramatically from a generic understanding of PHI in the current rule to the proposed rule's notion of any PHI in a "designated record set" (DRS) — essentially any PHI used to make a decision about a patient. In addition, providers would have to include disclosures made by all business associates that handle PHI. Many commenters pointed out a central flaw in HHS' proposed rule: not all information systems that hold PHI in a DRS log each access to patient records. Thus, the AR would potentially require modifications to many information systems within a provider and their business associates.

A common complaint from commenters was that there was little evidence that patients request and use AODs. The Medical Group Management Association found that only 6% of their members receive ten or more AOD requests per year [3], a very small number. Commenters argued that with such minimal use of the AOD by patients it made no sense to invest considerable resources to support the new AR.

3 Contextual Integrity and Disclosures

Frankly, it is hard to imagine patients interacting regularly and meaningfully with voluminous audit logs. The AR, as envisioned in the rule, would be a long list of time-stamped entries with names of the accessing user. Each line may also include a description of the PHI accessed and the user's action. For most patients, this sort of information is not particularly useful.

We approach this problem differently, from the perspective of contextual integrity [6] and ask instead: What do patients care about? What do they want to know about access to their PHI? What will patients do with the information about the flow of their PHI?

Contextual integrity views the central concern about privacy to be about appropriate flows of personal information. 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 provide rules prescribing information flows that are appropriate in given contexts. Flows that do not respect "appropriateness" violate contextual integrity and may constitute violations of privacy. In health care, some appropriate purposes would include the flow of PHI to ensure effective medical care, lower healthcare costs and improve health outcomes.

From the perspective of contextual integrity, our questions then reduce to: how do we give patients a better sense of PHI information flows?

4 Proposal: Accountings of Relationships

We propose a somewhat orthogonal artifact to the AOD, the "Accounting of Relationships" (AOR).

Where AODs and the proposed AR would provide detailed disclosure information about a patient, an AOR would instead aggregate data about information flows of PHI across all patients for a provider. That is, it would "flip" the focus for disclosure accounting from the individual patient to the covered entity.

The AOR we envision is a metadata-rich directed graph of data flows originating from the provider or their business associates to recipients of PHI. For a given provider, an AOR would describe all aggregated data flows about patients to external entities, including details as to senders and recipients and the general nature of the subjects of information flows. Each edge of such a graph would describe information such as how often this data is exchanged, how many patients per exchange per period are subject to a flow and what kinds of data were disclosed. AORs would need to be updated regularly and must be publicly available, such that providers could not claim that certain relationships of PHI data flows are proprietary relationships.

Providers should be held accountable for the accuracy of the information provided in AORs. The mechanism by which this might be achieved could be through the enforcement of self-regulatory codes, as the FTC proposes in its recent report on Protecting Consumer Privacy in a Era of Rapid Change [2]. The AOR should be a true aggregated representation of PHI data flows.

AORs would be data structures that patients should be able to use — with external tools — to compare data flow environments across organizations; they would need to be provided in a standardized format for graphs, such as the Activity Streams[1] JSON standard.

We envision a number of use cases for Accountings of Relationships. AORs will allow general and detailed comparisons of the data flows centered on a covered entity. Patients should be able to use a visualization of the AOR — a map — to compare the gross data flows across two or more organizations. For example, a research and teaching hospital will look much different in terms of data flows than a rural hospital or small clinic. If patients are concerned about research uses of their PHI, they can assess directly how much an institution engages in those kinds of flows and decide where to seek care. Further, when a version of the AOD is available in electronic form, it will be possible to annotate AORs with specific information about a patient's flows — noting in which of the institutional flows a patient's PHI participates — and it would be possible to use the information in the AOR to enrich AOD entries with metadata about other parties involved in specific disclosure events.

Our proposal is not without challenges. Privacy itself may be a challenge in creating AORs for small facilities; if only a few patients have PHI in a particular data flow, it may be easy to infer sensitive information about those patients. Finally, capturing the data about flows to then produce a robust aggregate may be difficult. However, reasonably accurate estimates made in good faith should suffice.

Acknowledgements

NYU's work was supported by Grant Number HHS 90TR0003/01; it is solely the responsibility of the authors and does not represent the views of HHS.

References

[1] *Proposed Rule: HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act*, Department of Health and Human Services, 76 Fed. Reg. 31426-31449, (2011, RIN 0991-AB62).
[2] *Protecting Consumer Privacy in an Era of Rapid Change*, 2012, Federal Trade Comission. URL: http://ftc.gov/opa/2012/03/privacyframework.shtm.
[3] *Public Comment on Proposed Rule*, 2011, Medical Group Management Association. URL: http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0374.
[4] *Records, Computers and the Rights of Citizens*, 1973, United States Department of Health, Education and Welfare. URL: http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.
[5] Hall, J.L. and H. Nissenbaum, *Analysis and Recommendations Concerning HHS Notice of Proposed Rulemaking Covering Changes to Accountings of Disclosure*, 2011: Submitted to HHS Chief Privacy Officer, Joy Pritts. URL: http://josephhall.org/papers/sharps-pritts-letter.pdf.
[6] Nissenbaum, H.F., *Privacy in Context: Technology, Policy, and The Integrity of Social Life.* 2010: Stanford University Press.

[1] *See:* http://activitystrea.ms/