PatientPrivacyRights

Our mission is to restore patient control over personal health information

July 31, 2017

The thing to measure is not process, but **outcome**. The outcome must be assessed in terms of **rights**. Lacking a framing around outcome and rights, the Objectives introduce regulations in an environment where regulatory capture has already been a demonstrated problem for over a decade. Regulation and certification of process is failing.

As HHS creates the Interoperability Standards Measurement Framework for the healthcare industry and government health data holders, it must also ensure the Framework also measures patients' ability to easily exchange personal health data with whomever they choose. **Interoperability is predicated on patients' rights to easily obtain copies of all their health data** in EHRs and in all other hospital software systems that use personal data (financial and billing records, prescription, x-rays, etc). HITECH gave patients the right to easily obtain copies of all health data, in a form they choose. The HIPAA statute and regs set out a broad right to copies of PHI. The same outcome for patients as for industry and government means HHS must finally ensure that everyone in the US can easily get copies of PHI. Patients have the strongest motivation to ensure personal data is available for treatment and research, and to ensure the data are correct. **Outcome: Patients are first-class citizens in what data is accessible to us as well as which APIs are accessible for patient-directed exchange. In terms of process, the Framework must measure and value only interfaces that are also accessible for patient-directed exchange, using the same standard APIs as industry and government.**

There is no universal address space for digital information transfer like we have with postal address or fax. Nor is there a clean accounting or accountability to the subject (the patient) of the information being exchanged, **despite the right to an accounting for all disclosures of PHI from EHRs and all hospital datasets, as specified in HITECH, HHS has never released final regulations so patients can have at least some accountability and transparency about the use of PHI**. Personal information in digital form is stored, used, sold as PHI or as "de-identified"-and-sold by layers of intermediaries, starting with the institution, the EHRs and other institutional vendors, the "exchanges", the trust brokers, and the hidden data brokers of re-identifiable data. In the analog days, health data could not legally be sold in any form, not even prescriptions. Why must we accept this violation of the universal human and civil right to the privacy of our most intimate data in the digital future? In January, a survey of 12,090 adults' attitudes toward health technology found massive mistrust in US EHRs and HIT: 89% of patients withheld

P.O. Box 248 • Austin TX • 78767 Phone 512.732.0033 • Fax 512.732.0036 Email: privacy@patientprivacyrights.org
www.patientprivacyrights.org

important information from physicians.[1] Restoring patient trust in technology and physicians requires accounting for disclosures of PHI. Only when patients know which persons or entities use, sell, or disclose PHI—to which persons or entities, and for what purpose, will they be able to trust US health technology systems and willingly share PHI.

The outcome patients deserve is the right to a personal longitudinal health record that's independent of any particular institution and that controls and reports access to digital personal information no matter who the custodian is. Simply put, a lab, hospital, pharmacy, or practice cannot be allowed to store or use personal information unless that information is registered and accessible to any would-be longitudinal patient record provider that is willing to copy the information in its native form and then have it sealed or deleted. In other words, personal information flows in a way that's accessible and accountable to the patient or it doesn't flow at all, to anyone (including to public health and law enforcement registries with rare exceptions).

Access to native-form information is seen as a possible taking of the secret intellectual property of the EHR vendor that controls the patient-level information. The way for the EHR vendor to mitigate or avoid this risk is by providing a format that patients prefer to direct as part of their longitudinal health record. This represents an intellectual property compromise between the custodian of the personal data and the patient. The custodian cannot have secret intellectual property in how the data is stored and accessed but the custodian is not forced to accept any particular standards-based alternative, either.

The questions below are briefly answered from the perspective that what will be measured is outcomes rather than standards.

Comments to the specific questions:

1) Is a voluntary, industry-based measure reporting system the best means to implement this framework? What barriers might exist to a voluntary, industry-based measure reporting system, and what mechanisms or approaches could be considered to maximize this system's value to stakeholders?

> Yes and No. Voluntary reporting to the Government will be partially helpful, but is insufficient on its own. The most important stakeholder is the individual patient (or their authorized representative). The most efficient way to implement an outcome measure is to enable each citizen to be able to assess, should they choose, whether they have access to all of their data, from all data holders. Their potential assessment thus necessarily requires that standards also be focused on provenance and transactional information, like that already legally required of individuals' financial data, and which was required in the Paper Age. Unless this Proposed Framework requires standards for additional reporting to each patient directly, accountability for their individual, legal rights is impossible. Moreover, disparate international standards will make the assessment of voluntary compliance with all individual rights practically impossible.
>
> Our nation was expressly founded to protect our citizens' individual rights. A "reasonable expectation of privacy, " rights to non-discrimination, and related due process are protected by the Fourth, Fifth, Ninth, Tenth and Fifteenth Amendments to the U.S. Constitution, and numerous State Constitutional provisions. Other federal statutes (in addition to HIPAA), such as

[1] URL: https://blackbookmarketresearch.newswire.com/news/healthcares-digital-divide-widens-black-book-consumer-survey-18432252

the Privacy Act of 1974, 5 U.S.C. Sec. 552a; the Fair Credit Reporting Act of 1970, 15 U.S.C. Sec. 1681; the Identity Theft and Assumption Deterrence Act of 1999, 18 U.S.C. Sec. 1028; and the Genetic Information Nondiscrimination Act, 42 U.S.C. Sec. 2000, among others, elucidate such rights. The new 21st Century Cures Act, (Pub. L. No. 114-255, 130 Stat 1033 (2016)), Section 4006, also requires the Secretary of Health and Human Services to promote policies ensuring that patients have access to their electronic health information. Many State laws (too numerous to list here) also require that many individual citizens be permitted to independently assess whether their individual rights have been violated.

Finally, access to all individual data is also necessary to fulfill the individual's right to the highest attainable standard of health and non-discrimination enumerated in several ratified international agreements, including, but not limited to: the Universal Declaration of Human Rights; the World Health Organization Constitutional Agreement; and the Convention on the Rights of Persons with Disabilities. (See http://healthcare.procon.org/view.resource.php?resourceID=005996). Many future foreign patients from Canada and the European Union will also be protected by their stringent data protection laws when treated here (See, e.g., the new European Union, General Data Protection Regulation, (Regulation (EU) 2016/679)).

2) What other alternative mechanisms to reporting on the measurement framework should be considered (for example, ONC partnering with industry on an annual survey)?

Institutions subject to an enforcement action must be registered with a public registry.

3) Does the proposed measurement framework include the correct set of objectives, goals, and measurement areas to inform progress on whether the technical requirements are in place to support interoperability?

No. The ability for digital intermediaries to manipulate the standards process in response to regulation - regulatory capture - calls for an outcome and rights basis for enforcement.

4) What, if any gaps, exist in the proposed measurement framework?

Given the anti-trust protections of the standards process, data custodians collude to charge as much as possible for their new rent-seeking services. We must develop frameworks that resist regulatory capture and re-institute anti-kickback laws and laws to end industry collusion.

5) Are the appropriate stakeholders identified who can support collection of needed data? If not, who should be added?

No. The appropriate stakeholder is the patient-subject of the personal data under custodial control. They must have a contemporaneous accounting for use and disclosure in the digital method of their choice (e.g: API, email, or text message). Access should be automated like electronic banking, with 24/7 access, and the ability to design notices of use/access and specify frequency and form of notices.

6) Would health IT developers, exchange networks, or other organizations who are data holders be able to monitor the implementation and use of measures outlined in the report? If not, what challenges might they face in developing and reporting on these measures?

This is related to the EU GDPR regulations going into force in 2018. GDPR is a good framework point for keeping custodians of personal data accountable. The choice of enforcement mechanism could be a combination of regulatory and legal sanctions.

7) Ideally, the implementation and use of interoperability standards could be reported on an annual basis in order to inform the Interoperability Standards Advisory (ISA), which publishes a reference edition annually. Is reporting on the implementation and/or use of interoperability standards on an annual basis feasible? If not, what potential challenges exist to reporting annually? What would be a more viable frequency of measurement given these considerations?

This should be no different from other public reporting registries operated by government agencies.

8) Given that it will likely not be possible to apply the measurement framework to all available standards, what processes should be put in place to determine the standards that should be monitored?

The framework should focus on outcome measures with OCR fines, patient and provider complaints and a “wall of shame” similar to data breach penalties as the measurements.

The framework should also measure what faction of all patient-level information is shared via patient-directed APIs as numerator and all patient-level information shared (including, for example, bulk interfaces, legacy HL7, and other means that are not patient-accessible or patient-directed) as the denominator.

9) How should ONC work with data holders to collaborate on the measures and address such questions as: How will standards be selected for measurement? How will measures be specified so that there is a common definition used by all data holders for consistent reporting?

ONC can certainly help through support of activities such as the HEAlth Relationship Trust (HEART) standards process that allows patient participation alongside industry-supported activities. ONC should only support totally open activities compatible with open source, community supported software. Vendor or software certification is a barrier to open source solutions and open source standards-based communities must not be disadvantaged in ONC-sponsored activities. In fact, open source solutions are far safer than proprietary IT solutions.

10) What measures should be used to track the level of “conformance” with or customization of standards after implementation in the field?

Amount of OCR fines, patient and provider complaints and a “wall of shame” need to be the principal measures; model the approach to fines after the very effective current system to address US health data breaches. What industries outside of healthcare track “conformance” to standards? Railroad gages? Building codes? Payments?

Signed,

Adrian Gropper, MD
Thomas Welch, JD
Deborah Peel, MD

P.O. Box 248 • Austin TX • 78767 Phone 512.732.0033 • Fax 512.732.0036 Email: privacy@patientprivacyrights.org
www.patientprivacyrights.org