



## **Incorporating Patient-Generated Data into Provider Electronic Health Records (EHRs)**

**Testimony of Deven McGraw, Director, Health Privacy Project  
Center for Democracy & Technology**

**Before the Health IT Policy and Standards Committees  
June 8, 2012**

Thank you for the opportunity to provide testimony on legal and policy issues associated with the incorporation of patient-generated data into electronic health records (EHRs). My testimony is based on my experience in serving on the Robert Wood Johnson Foundation's Project HealthDesign Regulatory and Assurance Advisory Group with the law firm Manatt, Phelps & Phillips, LLP, as well as my knowledge of the privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

You will hear testimony today from others associated with Project HealthDesign; each of the current Project HealthDesign grantees is incorporating some patient-generated data into clinical workflows. My testimony will not provide details on the five initiatives that comprise the current phase of Project HealthDesign; instead, I will describe some of the relevant legal and policy issues identified by the Project HealthDesign grantees at the start of their projects and how the grantees addressed them.

### Managing Liability Concerns Associated with Acceptance of Data Generated by Patients

A critical concern to the providers participating in Project HealthDesign was the potential for professional liability for failure to appropriately respond to data coming from a patient. Although providers have routinely accepted "data" reported by patients (either orally or in writing), most commonly in the context of an office visit, the concerns about potential liability increase when providers contemplate accepting electronic data that is routinely collected by patients and (potentially) routinely transmitted to clinicians. Among the concerns were the following:

- **Timeliness:** Are health care providers liable for critical/emergent clinical information once it is entered into a patient's PHR or sent to a health care provider through an EHR portal or e-mail? What if no one on the health care provider's staff sees the information right away?

- **Adequacy of Response:** What if a health care provider does not follow up on the information – either by seeking additional information or attempting to verify it? Do health care providers have an obligation to share information with specialists or others who health care providers who treat the patient?
- **Who Should Respond:** Are physicians liable for the failures of others (e.g., nurses and case managers) to respond to or accurately interpret electronic health data from patients?
- **Volume of Data:** What if the data that comes in through the PHR are not structured (and therefore cannot be automatically populated into clinically-relevant fields) and/or are so voluminous as to be overwhelming?
- **Accuracy:** How can health care providers trust the accuracy of patient-generated data? How can they ensure that data are not accidentally deleted or that the integrity of the data is not compromised after a patient transmits it?

Professional liability is determined by whether or not a provider followed the standard of care, which is driven by professional custom and an ever-evolving clinical evidence base. Models of care that involve the acceptance by providers of patient-generated data – particularly electronic data collected by the patient outside of an office visit or treatment episode – are still fairly rare. As a result, there is little guidance from professional liability case law about what constitutes the appropriate standard of care.

However, because of the potential for improved clinical outcomes and reduced costs due to more robust participation by patients in their own care, Project HealthDesign grantees all agreed that fears about potential professional liability should not become an obstacle to adoption of care models that include the acceptance of patient-generated electronic data. The standard of medical care has not yet evolved to the point where health care providers are routinely expected to receive electronic data generated by patients; but this standard is likely to evolve when practice patterns adapt to accommodate the new care delivery and payment models that depend on achieving favorable outcomes for patients.

The Project HealthDesign grantees found that easing the liability concerns of health care providers required **setting reasonable and realistic expectations on the part of both the clinical care team and the patient** that addressed each of the following questions:

- |               |   |
|---------------|---|
| <b>What:</b>  | What specific information should the patient share with his or her health care provider?  |
| <b>How</b>    | How should the information be formatted so that the health care provider can act on it? How will patients be educated about their rights and responsibilities?  |
| <b>Where:</b> | Where exactly should the information be collected (e.g., should the information remain on the patient-controlled device until it is accessed by the care team)? Under which circumstances, if any, will the information flow into the health care provider's EHR? |

**Who:** Who on the health care provider's staff should receive the information from the patient? To what extent should the information be shared with others? With whom should the information be shared if the information indicates a medical emergency?

**When:** When (how often and at what times) should a health care provider receive and review the information?

The Project HealthDesign grantee teams addressed the questions above as part of their research protocols. Thus, under each project, it was clear what type of data patients would be communicating, how they would do so, where the data would be stored and displayed, and which members of the clinical team would review the data, under what circumstances and how often. Thus, the "data flows" from the patient were tightly managed, and the plan for handling patient-generated data was tailored to the needs of each project.

In seeking to manage potential malpractice risk, the Project HealthDesign teams generally took one or more of the following steps:

- **Worked with patients to ensure that there was a common understanding of the types of information patients would be sharing with their health care providers, how the sharing would take place, which members of the clinical team would be reviewing the information and how often.** A number of the teams included these elements in their projects' informed consent forms, which each patient had to sign before they could participate in the project. Health care providers acting outside of a research protocol could document this common understanding through an agreement or compact signed by the health care provider and the patient. It is critical that the agreed-upon terms of the "deal" between the patient and the health care provider are consistently honored by all of the parties. If, for example, the parties agree that the patient should only e-mail the health care provider during business hours - and the patient e-mails after hours and the health care provider does not correct the behavior - the health care provider may not be able to rely on the "deal" to excuse an adverse incident.
- **Designated and trained a member of the health care provider's staff to monitor incoming data and triage as necessary.** Certain of the Project HealthDesign research teams learned that the most efficient way to incorporate patient-generated electronic health information into clinical care was to allow non-physician staff to view the information first. These staff members were able to communicate more frequently with patients, allowing physicians to review the information only when it was clinically necessary or as part of an office visit with the patient. For at least one grantee team, the patient generated data was used exclusively to improve the quality of the patient's narrative during the office visit.

Note that physicians may be held liable for the negligence of the members of their care team under the legal doctrine of "respondeat superior;"<sup>1</sup> therefore it is important that non-physician staff be well trained to appropriately review and respond to patient-generated data.

---

<sup>1</sup> *Franklin v. Gupta*, 567 A.2d 524, 537 (Md. Ct. Spec. App. 1990) (explaining that a physician can be held liable if "the negligent actors were, in fact, under his direct supervision and control").

- **Put a medical emergency protocol in place.** Grantees instructed patients to use traditional emergency communications channels in a medical emergency and not to expect that information communicated through a PHR or other tool would be reviewed on a real time basis by the health care providers participating in the research projects. Some teams also developed emergency communication plans that were triggered when non-physician staff members identified data that indicated the possibility of a medical emergency or the need for prompt clinical follow-up.
- **Used appropriate judgment in deciding when patient-generated electronic health information would be included in the health care provider's legal health record.** A health care provider's legal health record is "the documentation of health care services provided to an individual during any aspect of healthcare delivery in any type of health care organization."<sup>2</sup> While there is no one-size-fits all description of the contents of a legal health record, the purpose of the legal health record is to: support the decisions made in a patient's care; support the revenue sought from third-party payers; and document the services provided by the health care provider as evidence of the patient's illness or injury, response to treatment, and caregiver decisions.<sup>3</sup> **Patient-generated electronic health data did not automatically flow into the health care providers' EHRs under any of the projects.** Rather, the decision to include such information was either made in advance by the grantee teams or made by physicians on a case-by-case basis.

Project HealthDesign has demonstrated that more effective engagement of patients does not require providers to agree to open themselves up to a deluge of information from patients. Rather, health care providers can take steps to mitigate their liability risk, such as setting clear expectations about the types of information patients will share with providers, how the sharing should take place and which members of the clinical team will review the information and how often. Until a clear standard of care emerges, approaches like those adopted by Project HealthDesign grantees can enable health care providers to use patient-generated electronic data to deliver more patient-centered and, potentially, more effective and cost-efficient care.

#### Legal Treatment of Information Once it is Incorporated into a Provider's EHR

As noted above, providers and patients should collectively decide what and when patient-generated information will be submitted to the provider; providers should incorporate into their EHR any information that is relied on to make clinical treatment decisions, or that otherwise needs to become part of the legal medical record. That information should meet legal requirements for EHR documentation, which likely will require indication of the source of the information and meet other requirements to ensure data integrity. The mechanism for indicating source will likely depend on how the data is received by the clinician and incorporated into the record.

---

<sup>2</sup> Haugen MB, Tegen A, Warner D. Fundamentals of the legal health record and designated record set. J AHIMA. 2011 Feb;82(2):44-9.

<sup>3</sup> Id.

Once the information is part of the legal medical record, it should be treated by providers in the same way that other information in the record is treated. For example, under HIPAA, the information will be available to be accessed, used and disclosed for treatment, payment and health care operations without the need to obtain the consent of the individual, unless state or federal law expressly provides otherwise. It may be used for public health reporting or for research purposes, subject to the authorization and IRB/Privacy Board approval requirements of the HIPAA Privacy Rule. Patients have the right to a copy of it, and to request an amendment (and to submit rebuttal information if a provider decides not to grant the request for amendment.) Unless state law provides otherwise, the fact that the patient is the source of the information does not render it subject to a different set of rules than other information in the EHR. (CDT is not aware of any state law that provides special protections for data generated by patients and incorporated into a provider's EHR.) When clinicians and patients discuss the incorporation of patient-generated data in the EHR, patients should understand that this information, once incorporated into the provider's EHR, will be treated under the same confidentiality rules as apply to medical data created by the provider and his or her staff, and that it can be shared with others (including payers) in relevant circumstances.

#### Dealing with Security Issues

Providers have the responsibility under the HIPAA Security Rule to safeguard electronic PHI that is collected by, and maintained in, their EHR systems. Consequently, if a providers decides to directly connect to a patient to accept a feed of data into the EHR – such as by facilitating a connection to a medical device, or accepting a direct data feed from a patient's PHR – it is the provider's responsibility to ensure that the connection from the patient is authenticated and that the electronic connection doesn't introduce security risks into the provider's EHR.

Thank you for the opportunity to submit this testimony; I am happy to answer any questions you may have.