HIMSS Electronic Health Record Association

Statement of the Electronic Health Record Association (EHRA) before the Subcommittee on Privacy, Confidentiality & Security of the National Committee on Vital and Health Statistics

"Minimum Necessary and the Health Insurance Portability and Accountability Act"

Introduction

The Electronic Health Record Association (EHRA) is a trade association of electronic health record (EHR) companies, collaborating to address national efforts to create interoperable EHRs for use in hospital and ambulatory care settings. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care, as well as the productivity and sustainability of the healthcare system. On behalf of its member companies, the EHRA is pleased to provide this statement on the “minimum necessary” standard.

Existing Standards and Flexibility

The “minimum necessary” standard is a central aspect of the privacy rule that requires a covered entity to reasonably limit uses and disclosures of protected health information (PHI) to the minimum necessary to satisfy a particular purpose or carry out a function. The standard currently has some exceptions. As an example, it does not apply to disclosures or requests by a provider for purposes of treatment, with the amount of information being left to the provider’s discretion. This approach should be maintained. A health IT system cannot replace a provider’s judgment regarding the minimum necessary appropriate information.

Capability of Health IT Systems in Applying “Minimum Necessary”

For internal uses, health IT systems, such as EHRs, provide access controls to restrict access and use of PHI to authorized users in specific roles and individuals as determined by the healthcare provider. When a restriction is requested by the patient, or when additional protection is required based on the nature of the health service, technology solutions exist to support these requirements (e.g., tagging to provide the ability for health IT systems to filter clinical items based on the patient’s privacy preferences and only share information that is determined necessary and authorized). However, those protections are triggered by actions of the patient or the clinician, and are not initiated by the health IT system itself.

For example, Data Segmentation for Privacy (DS4P) is one initiative working on a complex problem, balancing the need for high quality information at the point of treatment with a patient’s right to privacy. The goal of DS4P is to provide a technical framework for providers to exchange sensitive information electronically by adding security and privacy labels to a clinical item or document, so that both sending and receiving systems can interpret and implement relevant controls accordingly. When sensitive health information is required to be shared, different solutions exist to implement “minimum necessary” through "computable privacy", including sharing patient consent bundled along with the information, using metadata tagging, or querying a central consent repository. However, prior to implementation of a technical solution, we urge attention to important policy issues surrounding this practice. The DS4P initiative has not yet studied the safety or medico-legal liability implications of use of the standard. A rigorous analysis in these areas will be essential to widespread adoption.

Use of technology to access data, such as application program interfaces (APIs), also provides additional abilities for health IT systems (EHRs, patient portals, mobile applications, etc.) to selectively query and share clinical information. Emerging standards, such as Fast Healthcare Interoperability Resources (FHIR), take a resource approach to the information model (medications, procedures, immunizations, etc.). This resource-based representation of clinical data elements also enables more granular queries and data sharing. FHIR also supports Representational State Transfer (REST), the software architecture style that forms the basis of the World Wide Web. As the health ecosystem expands and the need for information sharing grows, there is an increased need for systems to be interoperable, and emerging standards such as FHIR have garnered a lot of support from the software developer community to complement and expand on current interoperability capabilities.

Work in Progress

Existing capabilities of EHRs have successfully demonstrated implementation of “minimum necessary” through basic choice and access control. Emerging standards for granular access and granular patient choice are being piloted by several organizations. As the standards mature and more implementation guidance becomes available, we expect adoption to grow. The FHIR standard is currently in the draft stage, while DS4P as it currently stands has policy and process gaps – e.g., lack of a service discovery mechanism, lack of a standardized definition of sensitive health conditions, and the difficulty in navigating individual state laws – that must be addressed holistically in addition to solving the technical aspects of segmenting data. While DS4P provides the framework to tag at the section and clinical item level, managing access control at that level can create both operational and technical challenges. Handling one-to-many connections, where each endpoint may be different in terms of purpose of use, and resolving multiple consents and consent conflicts as the data flows through disparate systems, are still difficult problems that need to be resolved. Leaving the technical side out of the equation, there are real implications for patient safety when incomplete information is shared with other clinicians. Clinicians must also feel comfortable with the liability implications of making decisions based on incomplete data sets, and that doing so does not jeopardize their trust in or reliance on data from other sources.

The optional inclusion of DS4P in the 2015 meaningful use certification edition and the requirement for EHRs to support APIs indicates the Office of the National Coordinator for Health IT’s (ONC’s) general support of the evolving standards. As the technical requirements become more mature, implementation guides are developed and commercially proven, and policy issues regarding safety and liability are addressed, then health IT developers will roll out this functionality more widely to our client communities. As this is done, it will be critically important to assess any unintended consequences that may occur from our technical solutions to privacy concerns.