Privacy Engineering Provenance

Adrian Gropper, MD
CTO, Patient Privacy Rights
January 16, 2015

Thank you for the opportunity to present a patient-centered perspective on data provenance.

Good provenance metadata enhances both security and privacy. Your work on provenance can be a real-life example of privacy engineering or privacy by design in healthcare. Security is enhanced when assembled components of a patient's health record are traceable to the responsible party. This also reduces the cost of interoperability by reducing the risk of information intake by a care coordinator or medical home. Privacy is enhanced when ancillary services such as consumer apps or HIPAA Business Associates are prevented from abusing personally identifiable information. Good provenance technology is key to assembling a more comprehensive health record from both HIPAA and non-HIPAA data sources.

Apple HealthKit is one example of privacy engineering provenance and has already seen some adoption by institutions seeking to merge data from external patient-controlled services. The key to the HealthKit approach is a separate patient ID for each app or web service they connect to a patient account. This insulates the various service providers from each other, reduces Apple's risk in assembling highly personal information, allows more transparent control of data sharing by the patient, and ultimately makes the combined data more valuable to all. Good provenance metadata design saves money and improves health.

Provenance metadata is only as good as the patient ID. Patient ID is a difficult problem in healthcare and provenance inherits much of that difficulty. Privacy engineering allows us to make progress on provenance even as we continue to work on the broader problem of patient ID.

With respect to Question 1: Did the community miss something more impactful? I would note that provenance depends on three separate identities: the identity of the patient and at least two actors: the actor that ordered and provided a context for a test, and the actor that performed the test and provided a result back to the ordering actor. In all non-trivial cases, provenance metadata implies information about the identity of these three actors, the patient, the source and the reporter. Provenance metadata needs to bind these three actors together in a way that is both auditable and private.

With respect to Question 2, Where in the Use Case should the initiative start? Privacy engineering suggests that we start with Scenario 3 that includes an Assembler / Composer, where the Assembler can be the patient herself. If we can do provenance in that scenario, the other scenarios are easy. Combining safety, security, and privacy in Scenario 3 means that the Assembler / Composer can redact information about the patient but cannot merge

information from another patient. All of the result objects in the scenario 3 transaction must be guaranteed to pertain to the same patient even when the patient has had some tests performed under patient-controlled identifiers. The Assembler / Composer can be either an EHR or a PHR.

With respect to Question 3, Are there specific technology issues to consider? Assembling a combination of patient-generated data with data from trusted sources and locally generated data requires secure patient ID management by the Assembler / Composer. For example, Apple HealthKit, in the role of Assembler of information from multiple apps, does not share the patient's Apple ID with the apps. The patient is identified differently for each app and only the assembler is able to correlate the patient's information across multiple service providers. EHRs and PHRs will both benefit from this approach.

In summary, provenance can be designed to reduce the cost and risk of assembling data in an EHR or a PHR. Using cryptographic technology to bind the identity of the patient to the transaction will forestall the need for a general solution to the patient ID problem. Provenance linked to patient consent and accounting for disclosures will save money and improve health.