Patient Privacy Rights (PPR) API Task Force Testimony
January 28, 2016

I'm Adrian Gropper, Chief Technology Officer at Patient Privacy Rights. PPR is the world's leading health privacy advocacy organization. We represent a bipartisan coalition of 50 US organizations with 10.5 Million members and have 15,000 members. Patient Privacy Rights' mission is to restore patient control over personal health information.

To accomplish our mission, we educate and work collaboratively with patients and organizations to restore the ethical right to health information privacy, the foundation of the patient-physician relationship, in law, policy, and technology.

I am a medical software entrepreneur by trade, have contributed to a number of healthcare standards, and a co-founder of the HEART workgroup.

Patient Privacy Rights would like to address the major illegal gaps in today's systems that prevent patients from electronic access for second opinions, cost-effective treatment alternatives, and from donating health data for research and other uses.

Patient Privacy Rights' 5 key points:

1- A distinction between a patient-facing API and the FHIR API is unnecessary and undesirable. Patients have existing legal rights to full and equal access to personal data in EHRs.

2- HIPAA explicitly allows the patient to delegate direct access to their records and lab results; that includes access to second opinions by the licensed professionals of her choice.

3- With very limited exceptions, HIPAA says that the data that is accessible via other means will also be available through a patient-controlled API.

4- The HIPAA Security Rule, as applied to FHIR or to a patient-controlled API, could be used for "data blocking" by institutions. Data holders' that use security arguments to justify blocking patient-specified FHIR apps or clients are violating the law.

5- Potential security gaps can be fixed by appropriate encryption design of UMA, HEART, and FHIR so the unified Public API does not force a compromise between privacy and security.

The JASON reports and task force laid the foundation for the Public API. We must leverage the market forces behind FHIR and Argonaut to also improve access by patient-directed third parties.

As the recent OCR guidance makes clear, HIPAA gives the patient the right to have their health records and lab test results sent directly to a third party, even one that may be considered insecure or unwise by the covered entity or data holder. Paternalism is not legal. Unfortunately, the current guidance can force the patient into accepting an insecure transfer method such as un-

encrypted email or the use of a slower and less reliable method such as a Direct email attachment. A unified FHIR-based Public API should not force patients to choose between privacy (control over uses of PHI) and security.

At the patient-level, the content of a FHIR API for providers and patients is substantially the same. Patient safety requires that clinicians are able to bypass policy-based delays on the patient-directed API. Patients expect real-time access.

Data blocking will continue as long as covered entities and health data holders control which API apps or clients are “safe” under the HIPAA Security Rule. FHIR, HEART, and this Task Force must end the paternalistic, illegal blocking of patient access to EHR data and lab test results.

The OAuth privacy and security technology underlying FHIR and HEART is the best solution for patients and industry. As discussed in the Joint HIT Committee, a patient-specified third-party web service destination, cannot be blocked on account of HIPAA Security grounds. FHIR and HEART should be harmonized to enable a Public API by applying privacy engineering now, while the standards are still immature. PPR welcomes the opportunity to work with industry, government, and providers to ensure that data follows the patient without compromising data security.

Thank you,

Signed,

Deborah C. Peel, MD - Founder, PPR
Adrian Gropper, MD - CTO, PPR