

Patient Privacy Rights' 5 key API points:

- 1- A distinction between a patient-facing API and the FHIR API is unnecessary and undesirable.
- 2- HIPAA explicitly allows the patient to delegate direct third-party access to their records and lab results.
- 3- Per HIPAA, the designated record set 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 misused for “data blocking” by institutions.
- 5- Potential security gaps can be fixed by appropriate protection design of UMA, HEART, and FHIR so the unified Public API does not force a compromise between privacy and security.