**eCR Exchange Transactions**

Electronic Case Reporting (eCR) is the automated generation and transmission of case reports from the electronic health record (EHR) to public health agencies for review and action. It involves the interorganizational exchange of personally identifiable information (PII). It can involve exchange between many clinical care sites / EHRs for each Public Health Agency (PHA) or with one shared services platform as is in use by the Association of Public Health Laboratories (APHL) to support routing and processing for many PHAs. Health Information Exchange organizations (HIEs) can also, at times, be involved in these exchanges and are, in some cases, required by law to be used. Health Data Networks (HDNs) like the eHealth Exchange, Carequality, CommonWell, and DirectTrust also may play important roles.

eCR conceptually includes at least four interorganizational transactions:

1. The distribution of trigger codes / decision logic to guiding reporting
2. The reporting of electronic Initial Case Report (eICR) data from clinical care to an intermediary or a PHA
3. The delivery of Reportability Response information back to Providers/Reporters and/or EHR System Administrators
4. The capture of supplemental case reporting / investigation information

Transaction #4 is the least mature in this guide, but should be considered in respect to potential transactions and transaction security related issues.

**Requirements**

* Transaction #1 involves the delivery of publicly available, non-sensitive information. Whether it is the download of a trigger code spreadsheet (available on PHIN VADS) or the multi-channel (SMS, email, RESTful download, etc.) trigger / decision rule distribution possibilities of a FHIR value set subscription service, it is desirable to have user’s identity for subscription communication purposes, but extensive security to protect the data themselves is not necessary.
* The implementation of existing CDA transactions (the eICR and Reportability Response) can be supported by secure store-and-forward, push, and other exchange technologies. For these transactions, they could be point-to-point, could use an HIE, and could use an HDN.
* The data included in the eICR were identified by the Council of State and Territorial Epidemiologists (CSTE) electronic Initial Case Report Task Force. These data represent a HIPAA designated “minimum necessary” data set to carry out the needs of electronic case reporting. In this implementation guide the data are represented using a FHIR Composition resource and in the final IG they will also be bundled into the FHIR document paradigm.
* Standards solutions should support the secure connection of multiple clinical care sites / EHRs to a shared services platform and/or individual PHAs. While security levels for PHAs vary at times, the shared platform generally seeks to meet FISMA-level security expectations with its trading partners.
* The eICR being sent from clinical care to public health and the Reportability Response that goes back to clinical care both contain Personally Identifiable Information (PII) and need to be exchanged with very robust security considerations.
* The supplemental data in transaction #4 are typically are not found in EHRs as part of care. As such they may be supplemental data manually entered into web forms though standards like IHE RFD / HL7 SDC. While the eICR and the Reportability Response may pass through intermediaries, supplemental data are more likely to be manifest in a point-to-point solution. Some PHAs consider the posting of a web form not to need extensive transport security.

**Questions**

1. We believe that several different interorganizational exchange methodologies will be supported with FHIR as well as CDA. As such, while RESTful transactions should be supported, the eICR and Reportability Response FHIR data specifications should be loosely coupled to transport standards for some time. Are you aware of examples of external organizations, like PHAs, performing RESTful queries into EHRs or other clinical care server systems on a regular basis? If so, what is the context and what type of security is used?
2. Aside from RESTful GET (potentially in both directions) and RESTful POST/PUT, what transactions are you planning on supporting for interorganizational exchange with FHIR infrastructure?
3. If you work with Federal IT systems, do you believe that OpenID and OAuth 2 would pass Certification and Accreditation / Security Assessment and Authorization, and would it be found to be FISMA compliant? Are there other standards you would recommend that would be better?
4. Are there current FISMA compliant security technologies that can be applied at nationwide or State-wide levels that do not require mutual TLS, managed directories of providers / clinical care sites, and / or digital client certificates for the interorganizational exchange of PII?