

Privacy by Design Workshop

Privacy Use Case Template v.10

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Healthcare Use Case – Provenance – Data Source 🡪 End Point**

2. **Category of Use Case**

*Healthcare Data Provenance – Single Author*

3. **Provide a general description of the Use Case**

This use case focuses on a simple transmission of information from one healthcare provider to another healthcare provider. The information being sent has only one data source (i.e. there is only one author and the information is not being combined with any other existing information prior to transmission.)

End Point

(EHR)

Data Source

(EHR, Lab, Other)

*User Story 1: A patient is referred to an ophthalmologist by his primary care provider (PCP) for an eye exam. After the patient arrives at his office, the ophthalmologist conducts an eye exam and records all of the data in his EHR. The ophthalmologist electronically sends the information back to the patient’s PCP (where all data in the report sent was created by the ophthalmologist).*

*User Story 2: A patient wishes to transmit the Summary of Care Document she downloaded from her PCP to her Specialist. Rather than downloading and sending it herself, she requests[[1]](#footnote-1) that the PCP transmits a copy of the document on her behalf to her Specialist. PCP is the only author of the Summary of Care Document and also the sender of the information to the Specialist. The Specialist understands from the document’s provenance that it is authentic, reliable, and trustworthy.*

**…and Provide a summary inventory for the Use Case, including:**

4. **Application(s) associated with Use Case**

* Data Source EHR
* End Point EHR
* Transmission vehicle (Direct, FHIR)
* Billing application? (not part of current use case. Could be part of an expanded use case.)
* Patient Portal? (not part of current use case based on the assumption that requests are made in-person.)

5. **Data subject(s) associated with Use Case**

* Attending healthcare practitioner who is the only author of the information entered into the EHR.
* Data entry clerk entering the information into the EHR?(as written, there is no other data entry clerk other than the attending healthcare practitioner.)
* Patient, patient advocate, or guardian
* End point recipient(s)
	+ Primary healthcare practitioner
	+ Specialist
	+ Insurance? (as currently written, insurance is not a player in this use case.)

6. **Domain Owners, Domains, and Roles associated with Use Case**

 *[A “Domain Owner” is the Participant responsible for ensuring that privacy controls and PMRM services are managed in business processes and technical systems within a given Domain. A “Domain” includes both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner. “Role” includes the responsibilities assigned to specific Domain Owners within a privacy domain.]*

* **Domain 1:** Data Source EHR
	+ **Domain 1 Owner:** Data Source Healthcare Practitioner
	+ **Role:** Authors the information. Enters the information into the EHR. Initiates the transmission of the information to the end point.
* **Domain 2:** End point
	+ **Domain 2 Owner:** End Point Healthcare Practitioner.
	+ **Role:**Receives the transmitted data into their copy of the patient’s EHR
* **Domain 3:**Transmission vehicle? (Direct? FHIR? Trust Framework (Security Certificate Authority/Provider)? Too many variables at this point. Will elaborate later…)
	+ **Domain 3 Owner:** (TBD)
	+ **Role:** Transmit data between Domain 1 and Domain 2
* **Domain 4:**EHR developers?
	+ **Domain 4 Owner:** Any EHR development organization
	+ **Role:**Incorporate privacy, security and provenance capabilities into their EHR application.
* **Domain 5:**Patient Portal? (not part of current use case based on assumption)
* **Domain 6:**Insurance Company Portal (not part of current use case. Could be part of expanded use case.)

7. **Systems and products supporting the Use Case applications**

*[System is a collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management. Products are Categories of outputs or files containing PI or PII within the use case]*

* Domains 1 & 2: EHR systems at both ends of the transmission
* Domain 3:
	+ Internet service provider network?
	+ Trust Framework (Security certificate authority/provider)

8. **PI, PII, and PHI covered by the Use Case**

*[Specify the PI and PII collected, created, communicated, processed or stored within Privacy Domains or Systems]*

* Domains 1 & 2:
	+ Patient name, address, medical record number (SSN), Patient ID#, etc…
	+ Healthcare provider information
	+ Health information (diagnosis, treatment plan, lab test results, etc…)
	+ Insurance information
	+ Patient consent directive(s) (consent to treat or consent to disclose)(?)
	+ Handling caveats (?)
* Domain 3:
	+ All of the above information, encrypted.
	+ Header information (Origination information, destination information, subject line information)
	+ handling caveats (?)

**[Note: per domain, system, application or product, depending on level of use case analysis**

9. **Data Flows and Touch Points Linking Domains or Systems**

*[Touch points are the points of intersection of data flows with privacy domains or systems within privacy domains. Data flows are data exchanges carrying PI and privacy policies among domains in the use case Provide a simple diagram showing the touch points applicable to the Use Case]*

End Point

(EHR)

Data Source

(EHR, Lab, Other)

10. **Legal, regulatory and /or business policies governing the Use Case**

*[Define and describe the source of policies and regulatory requirements governing privacy conformance within use case domains or systems]*

* HIPAA Privacy and Security rules
* HIPAA Patient Right of Access
* Federal Privacy Act
* EHR meaningful use requirements
* Healthcare provider’s policies (could be more stringent than Federal Laws or regulations)
* State Privacy laws
* Patient consent to disclose directives

11. **Privacy controls required within the Use Case**

*Control - a process designed to provide reasonable assurance regarding the achievement of stated objectives*

* NIST SP800-53, Appendix J, Privacy Control Catalog

|  |  |
| --- | --- |
| **ID**  | **PRIVACY CONTROLS**  |
| **AP**  | **Authority and Purpose**  |
| AP-1  | Authority to Collect  |
| AP-2  | Purpose Specification  |
| **AR**  | **Accountability, Audit, and Risk Management**  |
| AR-1  | Governance and Privacy Program  |
| AR-2  | Privacy Impact and Risk Assessment  |
| AR-3  | Privacy Requirements for Contractors and Service Providers  |
| AR-4  | Privacy Monitoring and Auditing  |
| AR-5  | Privacy Awareness and Training  |
| AR-6  | Privacy Reporting  |
| AR-7  | Privacy-Enhanced System Design and Development  |
| AR-8  | Accounting of Disclosures  |
| **DI**  | **Data Quality and Integrity**  |
| DI-1  | Data Quality  |
| DI-2  | Data Integrity and Data Integrity Board  |
| **DM**  | **Data Minimization and Retention**  |
| DM-1  | Minimization of Personally Identifiable Information  |
| DM-2  | Data Retention and Disposal  |
| DM-3  | Minimization of PII Used in Testing, Training, and Research  |
| **IP**  | **Individual Participation and Redress**  |
| IP-1  | Consent  |
| IP-2  | Individual Access  |
| IP-3  | Redress  |
| IP-4  | Complaint Management  |
| **SE**  | **Security**  |
| SE-1  | Inventory of Personally Identifiable Information  |
| SE-2  | Privacy Incident Response  |
| **TR**  | **Transparency**  |
| TR-1  | Privacy Notice  |
| TR-2  | System of Records Notices and Privacy Act Statements  |
| TR-3  | Dissemination of Privacy Program Information  |
| **UL**  | **Use Limitation**  |
| UL-1  | Internal Use  |
| UL-2  | Information Sharing with Third Parties  |

[Note: to be developed against specific domain, system, or applications as required by internal governance policies and regulations]

12.  **Functional Services Necessary to Support Privacy Controls**

*Service - a collection of related functions and mechanisms that operate for a specified purpose*

* HL7 Security and Privacy Labeling Service Requirements
* Federal Bridge Certified Certificate Authorities or Trust Bundles (if they want/need to communicate with a federal health provider such as VA or DoD. May be required for Medicare patients.)

1. *Assumption: the patient’s request is made in-person as opposed to by phone, email or patient portal.* [↑](#footnote-ref-1)