Privacy Requirements Definition and Testing in the Healthcare Environment

Julie S. McEwen, CIPM, CIPP/G/IT/US, CISSP, PMP
Julie Snyder, CIPM, CIPP/G/US

Health in the 21st Century

Follow us on Twitter
MITREHealth

MITRE

Approved for Public Release. Distribution Unlimited. 13-2766

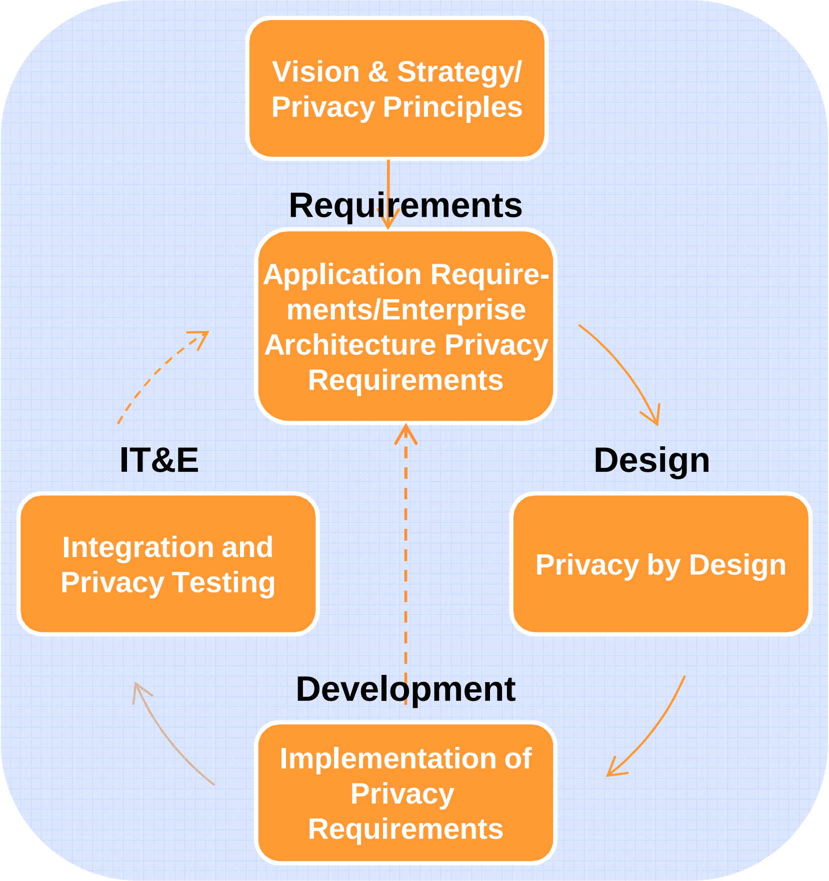
Problem

- Privacy laws and regulations articulate many privacy requirements at an abstract level
- It can be challenging for system developers to translate these requirements into system and application characteristics
- “Privacy testing" refers to specific system tests that are performed to ensure that privacy requirements are implemented correctly in systems.
  - This is an important step to ensure that systems appropriately protect Personally Identifiable Information (PII).
  - Privacy testing is especially vital for systems that process large amounts of Protected Health Information (PHI) to reduce the likelihood of errors in care and fraud, and reduce the overall cost of error in providing healthcare services.
- *However, there has not yet been a broader effort to articulate privacy requirements at the system/application level and address using privacy testing to verify that basic privacy controls are correctly implemented within the healthcare environment.*

Privacy Requirements Definition and Privacy Testing Are NOT Separate Processes

- Approach
  - Integrate privacy requirements definition and testing activities into the existing system development process
  - Have privacy testing as a rigorous and explicit activity in the system testing process
  - Privacy testing is fundamentally the same as other types of testing performed on the system – it just has a privacy focus

Privacy Testing as Part of Overall System Development Process


Vision & Strategy/ Privacy Principles
Requirements
Application Require-ments/Enterprise Architecture Privacy Requirements
IT&E
Design
Integration and Privacy Testing
Privacy by Design
Development
Implementation of Privacy Requirements

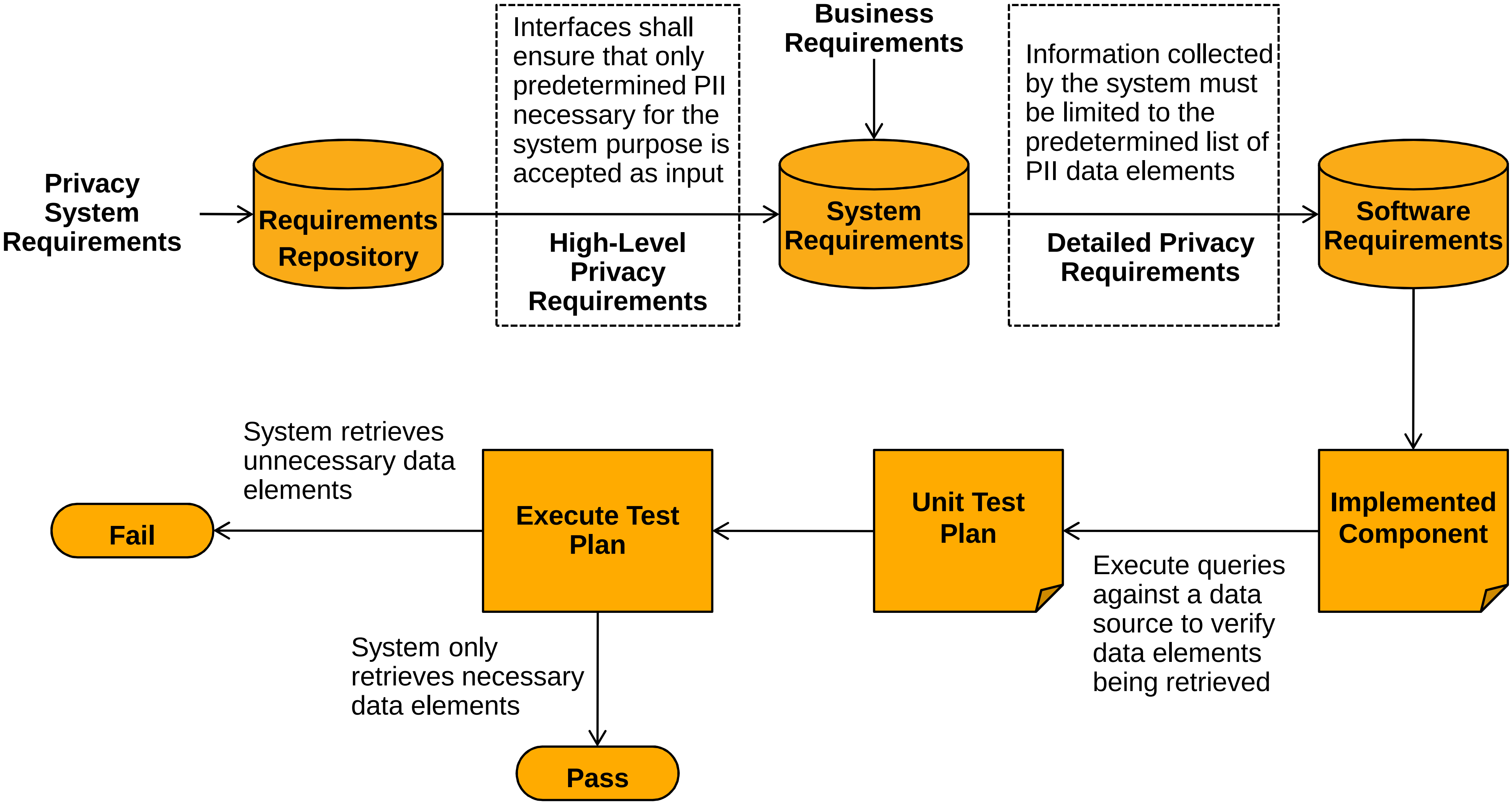
Objective: Expand testing to ensure privacy is enforced throughout the system's development life cycle

Idea

- **Engage with standards bodies to include healthcare-related privacy requirements and tests in standards and guidance documents that are used by the healthcare industry.**
  - **Goal is to promote broad adoption of privacy testing activities within the healthcare industry.**
- **Revise the existing MITRE privacy risk management tool (PRIME) so that it can be used for privacy requirements definition and testing efforts in the healthcare environment.**
  - **Goal is to make it easier for the healthcare industry to integrate privacy testing into their existing system testing processes.**
  - **PRIME is becoming open source, which will make it easier for the tool to be adopted for use within the healthcare environment.**

From Privacy Requirement to Privacy Test Results

Example: PII Minimization


Privacy System Requirements
Requirements Repository
Interfaces shall ensure that only predetermined PII necessary for the system purpose is accepted as input
High-Level Privacy Requirements
Business Requirements
System Requirements
Information collected by the system must be limited to the predetermined list of PII data elements
Detailed Privacy Requirements
Software Requirements
Implemented Component
Execute queries against a data source to verify data elements being retrieved
Unit Test Plan
Execute Test Plan
System retrieves unnecessary data elements
Fail
System only retrieves necessary data elements
Pass

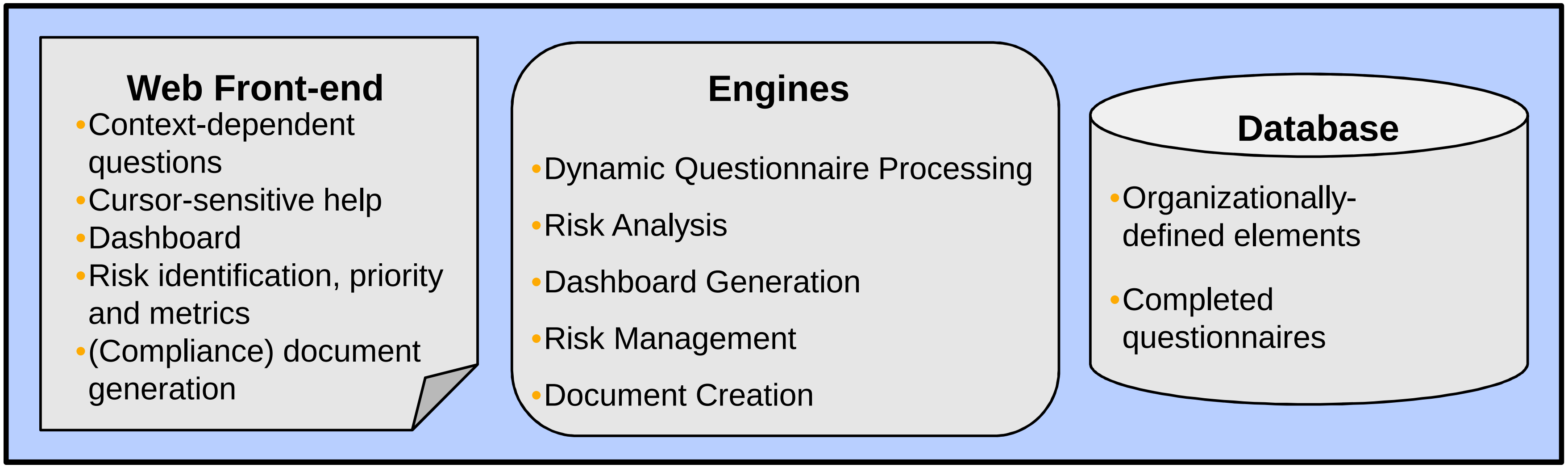
Sample Privacy Requirements, Tests, & Verification Methods

NIST 800-53 Rev 4 App J Requirement	HIPAA Privacy Rule	High-Level Privacy Requirements	Detailed Privacy Requirements	Privacy Tests/Verification Methods
CONSENT				
IP-1(d): The organization: Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	45 C.F.R. §164.502(c) implies consent is obtained 45 C.F.R. §164.522	Systems that directly interface with individuals shall distinguish between mandatory and voluntary PII collection.	For systems that collect PII from sources other than the individual, the system shall support a method of tracking consent when appropriate.	Create test record with the consent flag enabled and one with the consent flag disabled. Attempt to execute an action that requires use of the consent flag.
COMPLAINT MANAGEMENT				
IP-4: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	45 C.F.R. §160.306 45 C.F.R. §160.310 45 C.F.R. §164.530(d)(1)	The system shall support the tracking of disputed PII.	When the individual disputes the accuracy of PII or any output based on the disputed PII, the system shall maintain a flag indicating that the PII is in dispute.	Submit test PII to the system. Subsequently submit a dispute of the same PII.

Privacy Risk Management Engine (PRIME) Tool

- **PRIME is a web-based proof-of-concept tool that:**
  - **Provides modularized, organizationally tailored analysis.**
  - **Supports dynamic ‘drill-down’ risk analysis trees.**
    - **Discrete questions (yes/no, checkboxes, etc.) to simplify analysis**
    - **‘Drill-down’ questions are displayed if needed based on prior answers**
    - **Supports complex risk analysis to reduce false positives**
  - **Generates raw risk at different views.**
    - **Detailed: Risk level, risk description, risk mitigation suggestion**
    - **Program level: Risk thermometer with risk ‘temperature’**

PRIME Components



Web Front-end
- Context-dependent questions
- Cursor-sensitive help
- Dashboard
- Risk identification, priority and metrics
- (Compliance) document generation

Engines
- Dynamic Questionnaire Processing
- Risk Analysis
- Dashboard Generation
- Risk Management
- Document Creation

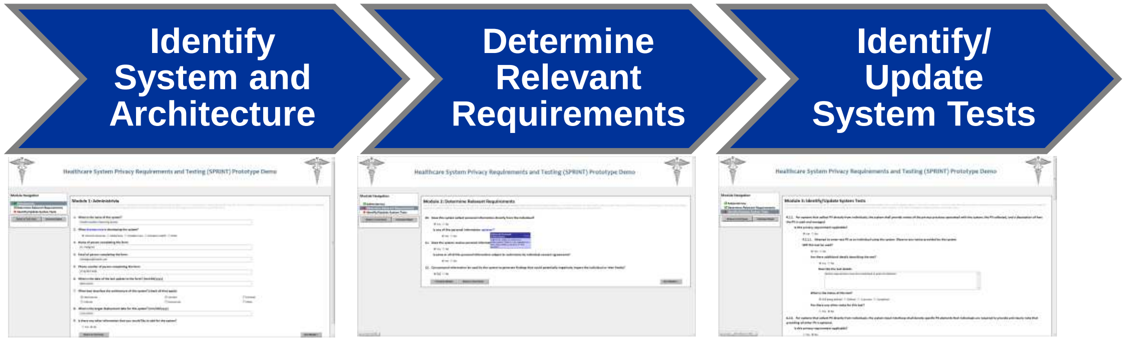
Database
- Organizationally-defined elements
- Completed questionnaires

Approach

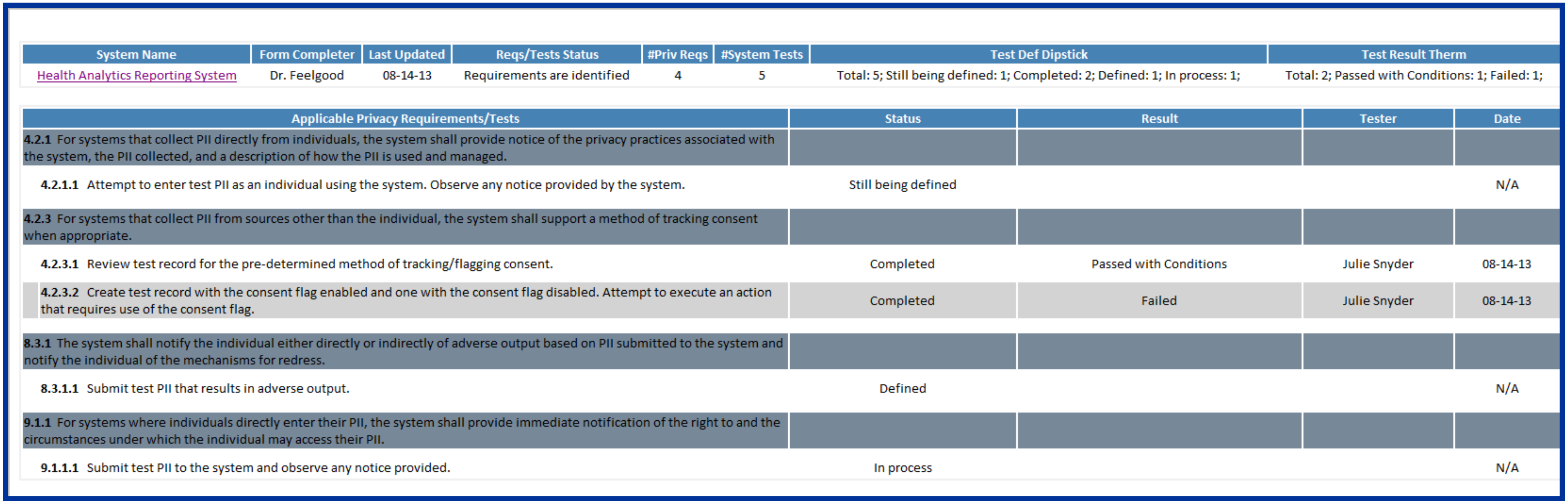
- Standards and guidance
  - Continue work to define system-level privacy requirements and privacy tests in guidance and standards
- Privacy testing tool
  - Add a healthcare instance to the existing MITRE proof of concept web-based PRIME tool so that it can be used within the healthcare environment to:
    - Select privacy requirements and privacy tests.
    - Document how tests will be performed and their results.
    - Document privacy risk decisions.
  - Engage with NIST and healthcare stakeholders to integrate the privacy tests into overall testing processes by adopting the use of the updated PRIME tool within the healthcare environment.

PRIME for Privacy Requirements and Testing → SPRINT

The Healthcare System Privacy Requirements and Testing (SPRINT) tool is built on MITRE's PRIME platform.


Identify System and Architecture
Determine Relevant Requirements
Identify/ Update System Tests

Sample System Privacy Testing Summary Report



System Name	Form Completer	Last Updated	Reqs/Tests Status	#Priv Reqs	#System Tests	Test Def Dipstick	Test Result Therm
Health Analytics Reporting System	Dr. Feelgood	08-14-13	Requirements are identified	4	5	Total: 5; Still being defined: 1; Completed: 2; Defined: 1; In process: 1;	Total: 2; Passed with Conditions: 1; Failed: 1;

Applicable Privacy Requirements/Tests	Status	Result	Tester	Date
4.2.1 For systems that collect PII directly from individuals, the system shall provide notice of the privacy practices associated with the system, the PII collected, and a description of how the PII is used and managed.				
4.2.1.1 Attempt to enter test PII as an individual using the system. Observe any notice provided by the system.	Still being defined			N/A
4.2.3 For systems that collect PII from sources other than the individual, the system shall support a method of tracking consent when appropriate.				
4.2.3.1 Review test record for the pre-determined method of tracking/flagging consent.	Completed	Passed with Conditions	Julie Snyder	08-14-13
4.2.3.2 Create test record with the consent flag enabled and one with the consent flag disabled. Attempt to execute an action that requires use of the consent flag.	Completed	Failed	Julie Snyder	08-14-13
8.3.1 The system shall notify the individual either directly or indirectly of adverse output based on PII submitted to the system and notify the individual of the mechanisms for redress.				
8.3.1.1 Submit test PII that results in adverse output.	Defined			N/A
9.1.1 For systems where individuals directly enter their PII, the system shall provide immediate notification of the right to and the circumstances under which the individual may access their PII.				
9.1.1.1 Submit test PII to the system and observe any notice provided.	In process			N/A

MITRE

Impact

Provide healthcare organizations with a tool that they can use to help implement Privacy by Design within the healthcare environment, thus enabling organizations to address privacy as systems are designed and developed.

MITRE