PrivacyeSuite v5.0

Consent Management / Computable Privacy

Challenge

Healthcare organizations, health information exchanges (HIEs) and jurisdictions face the challenge of electronically managing and enforcing individual, organizational and regional privacy consent directives while allowing appropriate access to protected health information (PHI) in support of patient care. Reinvigorated random audits by the Office for Civil Rights (OCR) and exposure to internal data breaches plague their organizations.

Regulations governing mental health and substance abuse, and initiatives such as medications management programs that seek to mitigate a consumer practice of "doctor shopping," need to address PHI privacy. Moreover, sensitive sexual health information remains an area of privacy concern for the healthcare consumer.

Electronic communication across diverse healthcare delivery systems requires a computable solution that:
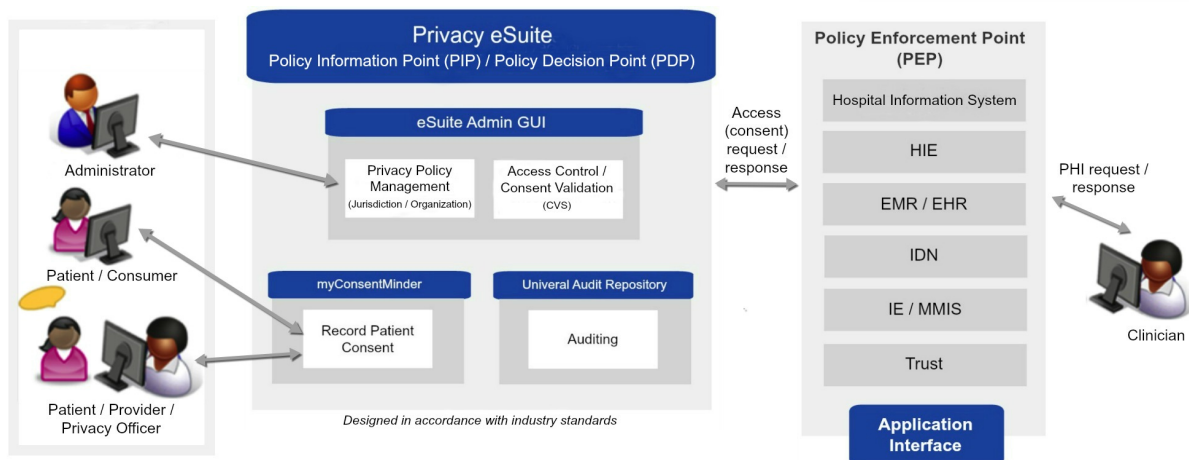
1. Leverages structured data to achieve end-to-end automated electronic consent management.
2. Uses industry standards to interoperate in an HIE ecosystem occupied by a multitude of EHR systems.
3. Processes complex rule-sets governing different consent at various levels, including organizational, regional, state and federal.
   (HIPAA/ HITECH, 42 CFR Part II, NIST SP 800-53r.4 [Appendix J])
4. Audits access – and attempted access – to all protected health information.

Solution

Consent management / computable privacy goes beyond role-based access control to address the *appropriateness* of access to PHI.

Privacy eSuite (PeS) is a web services-based consent engine developed to enable organizations, HIEs and jurisdictions to electronically manage, enforce and audit complex health information privacy policies in a diverse EHR ecosystem.

Designed in accordance with industry standards

Government Initiatives:

Privacy eSuite v5.0

Benefits of Centralized Consent Management	- Consistent, interoperable privacy capabilities for all systems, with minimal integration - The burden of adjudication for appropriateness of access to PHI is removed from point-of-care systems - Modifications to access control policies are made network-wide in near-real time - Designed to minimize "alert fatigue;" virtually no impact to workflow
Key Features of Privacy eSuite	- Allows providers, organizations and jurisdictions to proactively manage privacy - Accommodates the consent policy of virtually any jurisdiction - Supports HITECH provisions for Accounting of Disclosures and Breach Alerts - Design permits a distributed model in cases of multi-state/organization interaction - Enables granular, standards-based consent policies that accommodate: - Purpose of use: treatment, research, marketing, etc. - Information type: laboratory results, radiology exam, medication, etc. - Specific user(s): roles, groups of users, facility, etc. - PHI identifiers: category codes, classification codes, etc. - Supports Privacy by Design (PbD) principles

Where PeS Fits

Privacy eSuite operates at the middle tier as a rules engine to centrally manage and help enforce health information privacy policies established by consumers, organizations and jurisdictions. It provides the decision point for balancing PHI privacy against clinical access to health information. Balance is achieved through Break-the-Glass/Override functionality, which includes an immediate notification of a potential breach to a designated individual, i.e. compliance officer.

Privacy eSuite v5.0 - HIE/Jurisdictional Deployment
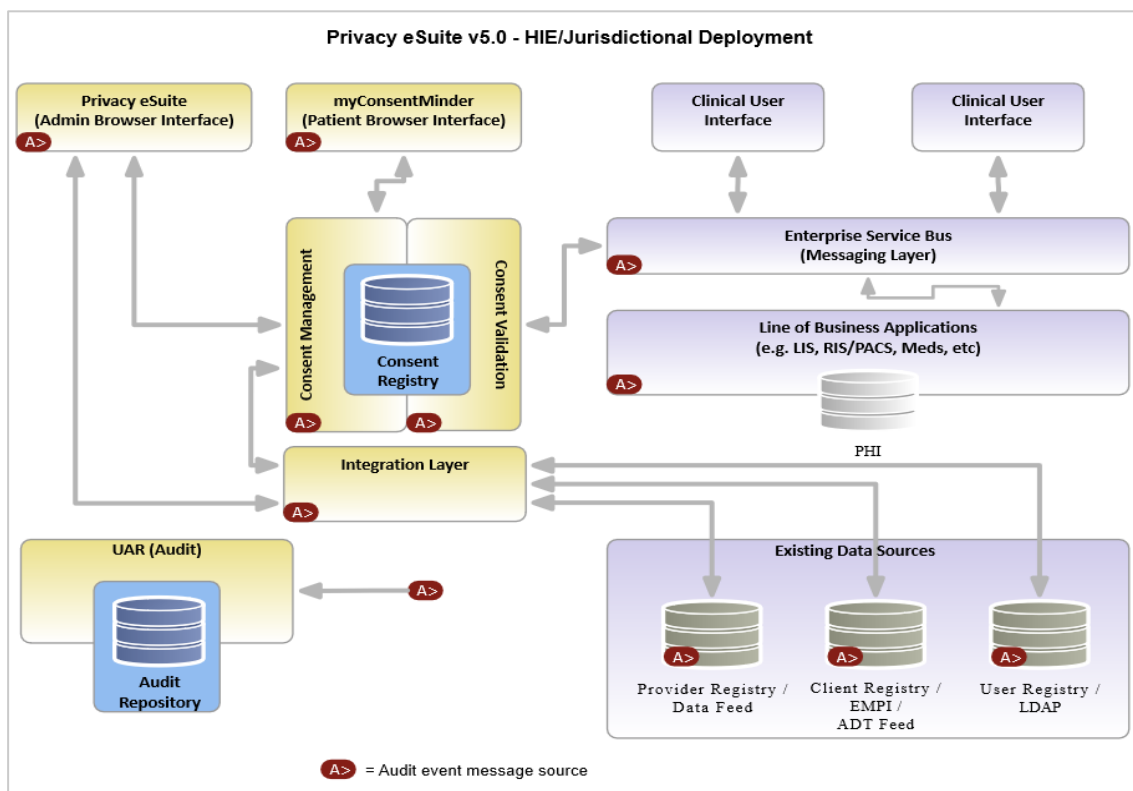
Standards Supported

HL7 Composite Security & Privacy Domain Analysis Model
HL7 CDA R2
IHE ATNA
IHE XDS.b
OASIS XACML v3.0
OASIS XSPA v1.0

myConsentMinder	A web-based, end-user-facing application (patient or clinician) to capture privacy preferences with simple preconfigured templates created through PeS.
Consent Management Service (CMS)	The CMS enables privacy policies to be administered and processed into computable access rules.
Consent Validation Service (CVS)	The high-speed CVS determines if user access to a patient's PHI is appropriate based on the rules of the existing privacy policies.
Universal Audit Repository (UAR)	The UAR is the IHE ATNA-compliant central audit repository that tracks audit events related to updates, queries, and retrieval access to PHI.