JOURNAL OF HEALTH CARE FINANCE

Spring 2021

SECURITY AND PRIVACY OF THE INTEGRATED CLINICAL ENVIRONMENT PART III

JASON LEE WILLIAMS, MSIT, JD, LLM, CIPP/US

INTRODUCTION

Integration without security and privacy is not interoperability. The integrated clinical environment cannot achieve patient safety goals, increase treatment effectiveness, and improve operational efficiency without engineering both privacy and security into clinical systems, institutional health information systems, and health information exchanges.

Security and Privacy of the Integrated Clinical Environment is a series of three articles. Part I discussed the basic concepts of interoperability and the integrated clinical environment (ICE), the legal and regulatory framework impacting an interoperable ICE, and an overview of the risks of deploying an interoperable ICE. The second article discussed the concept of privacy engineering and the various National Institute of Standards and Technology (NIST) frameworks and methodologies, including the new NIST Privacy Framework, that can be utilized to address both privacy and security risk adequately. The third and final article will discuss how the SABSA methodology can be leveraged to integrate privacy and security management throughout the interoperable, integrated clinical environment.

SABSA – AN ARCHITECTURE TO INTEGRATE FRAMEWORKS

"The purpose of security is to enable opportunities and mitigate threats so as to optimize business performance."[1] The SABSA methodology can be expanded to address both privacy and security concerns. Although designed as security architecture, SABSA provides a method to integrate privacy and security management with one overall architecture.[2]

A. *Introduction to SABSA Methodology and Health Care Integration:*

"Security architecture should result in the creation of security systems, practices and services that enable business success."[3] The SABSA methodology can be leveraged to build an architecture from the NIST frameworks that enable health care organizations to engineer information systems that will allow integration and interoperability while protecting patient privacy and information security. The concept of an interoperable, integrated clinical environment must be formed into an architecture that is both compliant, secure, private, and beneficial to the patient, the clinical staff, health care operations, and the general public.[4] "The purpose of security

[1] THE SABSA INSTITUTE ACADEMIC BOARD, R101 SABSA MATRICES 2018 4 (June 2018) [hereinafter SABSA MATRICES 2018], https://sabsa.org/white-paper-requests/.

[2] In 2018, SABSA released an update to its matrices stating, "One of the driving forces behind the 2018 update has been to reflect the changes in SABSA Thinking™ that have broadened the applicability of SABSA to all aspects of enterprise architecture. Thus in some places the terminology has been modified to create this broader vision of applicability." *Id.* at 3.

[3] *Id.* at 4.

[4] *See generally*, U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTHCARE & PUBLIC HEALTH SECTOR COORDINATING COUNCILS, HEALTH INDUSTRY CYBERSECURITY PRACTICES: TECHNICAL VOLUME 1: CYBERSECURITY PRACTICES FOR SMALL HEALTH CARE ORGANIZATIONS (Dec. 2018), https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf; U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTHCARE & PUBLIC HEALTH SECTOR COORDINATING COUNCILS, HEALTH INDUSTRY CYBERSECURITY PRACTICES: TECHNICAL VOLUME 2: CYBERSECURITY PRACTICES FOR MEDIUM AND LARGE HEALTH CARE ORGANIZATIONS (Dec. 2018), https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf; U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTHCARE & PUBLIC HEALTH SECTOR COORDINATING COUNCILS, HEALTH INDUSTRY CYBERSECURITY PRACTICES: RESOURCES AND TEMPLATES (Dec. 2018), https://www.phe.gov/Preparedness/planning/405d/Documents/resources-templates-508.pdf; ASS'N OF INT'L CERTIFIED PROF'L ACCOUNTANTS, SOC 2® - SOC FOR SERVICE ORGANIZATIONS: TRUST SERVICES CRITERIA,

is to enable opportunities and mitigate threats so as to optimize business performance."[5] The same can be said of privacy; privacy must be viewed as an enabler of business objectives. A health care organization must be able to operate at the optimized level while still adequately addressing privacy and security risk. SABSA provides a methodology to balance competing business interests against privacy and security. A health care organization that is entirely secure and private could not effectively operate in an interoperable, integrated clinical environment. Risk can be controlled and mitigated but not completely eliminated.

Forming the proper context is essential to show how legal and regulatory issues might impact the conceptual theory of ICE and interoperability. However, the concepts of integration, interoperability, and legal and regulatory compliance must be developed into an architecture that supports business objectives. Architecture is most commonly associated with "the art or science of building."[6] However, architecture is also defined as a "formation or construction resulting from or as if from a conscious act . . .[or] a unifying or coherent form or structure."[7] Information systems architecture addresses the same issues as our conventional notions of architecture but applies to the systems and technology that an enterprise uses to share information.[8] The SABSA methodology provides the architecture necessary to manage the complexity inherent in an interoperable, integrated clinical environment.

The SABSA methodology utilizes six layers (views) of architecture, contextual, conceptual, logical, physical, component, and management, to facilitate creating a system that addresses risk while achieving business objectives.[9] Additionally, the six layers are divided into six subcategories of questions: assets (What are you trying to do?), motivation (Why are you doing it?), process (How are you trying to do it?), people (Who is involved?), location (Where are you doing it?), and time (When are you doing it?).[10] The SABSA methodology is best understood through the SABSA matrices.[11]

B. ***SABSA Contextual Architecture:***

Contextual architecture is the businessman's view of what business requirements need to be met by the architecture being built. The contextual architecture ensures there is a thorough

---

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html; INT'L ORG. FOR STANDARDIZATION. ISO/IEC 27002:2013 PREVIEW INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS (October 2013), https://www.iso.org/standard/54533.html.

[5] SABSA MATRICES 2018, *supra* note 1, at 4.

[6] MERRIAM-WEBSTER, DICTIONARY, ARCHITECTURE, https://www.merriam-webster.com/dictionary/architecture (last visited Mar. 15, 2021).

[7] *Id.*

[8] JOHN SHERWOOD ET AL., SABSA WHITE PAPER, ENTERPRISE SECURITY ARCHITECTURE 3 (2009) [hereinafter SABSA WHITE PAPER], https://sabsa.org/white-paper-requests/.

[9] SABSA MATRICES 2018, *supra* note 1, at 7.

[10] SABSA WHITE PAPER, *supra* note 8, at 15.

[11] SABSA MATRICES 2018, *supra* note 1, at 7-8. SABSA provides an architecture matrix and a management matrix to guide professionals in using the SABSA methodology. SABSA identifies sixteen design principles for constructing the matrices: Business Driver, Risk Driven, Value Drive, Process Driven, Layered Traceability, Completeness, Justification, Architecture Design Artefacts, Management Activities, Dual Level Detail, and Table. *Id.* at 4-5. The design principles and matrices provide high-level guidance in using the SABA methodology. The matrices can be found at https://sabsa.org/white-papers/.

understanding of the requirements before the design begins.[12] The six subcategories of questions at the contextual layer are business goals and decisions (what), business risk (why), business meta-process (how), business governance (who), business geography (where), and business time dependence (when).[13]

C. *SABSA Conceptual Architecture:*

Conceptual architecture is the architect's view of the business requirements and the principles and fundamental concepts that guide the selection of elements at lower levels of abstraction.[14] The six subcategories of questions at the conceptual layer are business value and knowledge (what), risk management strategy and objectives (why), strategies for process assurance (how), security and risk governance, trust framework (who), domain framework (where), and time management framework (when).[15]

The SABSA Business Attribute Profile is a "requirements engineering technique that makes SABSA truly unique and provides the linkage between business requirements and technology/process design."[16] The business attribute profile is built at the conceptual layer and forms the core of the architecture describing each organization's unique set of business requirements.[17] The NIST Cybersecurity Framework (CSF)[18] and Privacy Framework[19] both require creating profiles to define requirements.[20] However, the NIST and SABSA profiles are different in how the profile impacts the overall architecture. The SABSA profile provides the link to the business requirements where the NIST profiles are used to manage risks identified by the organization. The different profiles complement one another but are developed and deployed at different levels of the architecture.

D. *SABSA Logical Architecture:*

Logical architecture is the designer's view of the business requirements and "models the business as a system, within system components that themselves are sub-systems."[21] The process

---

[12] JOHN SHERWOOD ET AL., ENTERPRISE SECURITY ARCHITECTURE: A BUSINESS-DRIVEN APPROACH 35 (2005).
[13] SABSA MATRICES 2018, *supra* note 1, at 7.
[14] JOHN SHERWOOD ET AL., *supra* note 12, at 37.
[15] SABSA MATRICES 2018, *supra* note 1, at 7.
[16] SABSA WHITE PAPER, *supra* note 8, at 19.
[17] *Id*.
[18] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY Version 1.1. 4 (Apr. 16, 2018) [*hereinafter* NIST CYBERSECURITY FRAMEWORK], https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[19] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0 8 (Jan. 16, 2020) [*hereinafter* NIST PRIVACY FRAMEWORK], https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.
[20] A high-level SABSA Business Attributes Profile can be found at JOHN SHERWOOD ET AL., SABSA WHITE PAPER, ENTERPRISE SECURITY ARCHITECTURE 21 (2009), https://sabsa.org/white-paper-requests. The NIST Privacy Framework Core and CSF Framework Core also provide profiles. *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 18, at 24 - 44; NIST PRIVACY FRAMEWORK, *supra* note 19, at 20 - 27; The general concept of generating profiles is shared between the NIST frameworks and SABSA; however, the SABSA methodology requires the architecture to create links between business requirements and information technology and process. SABSA WHITE PAPER, *supra* note 8, at 19.
[21] JOHN SHERWOOD ET AL., *supra* note 12, at 37.

used during the logical architecture phase is commonly known as systems engineering.[22] The six subcategories of questions at the logical layer are information assets (what), risk management policies (why), process maps and services (how), trust relationships (who), domain maps (where), calendar and timetable (when).[23]

E. *SABSA Physical Architecture:*

Physical architecture is the builder's view of how the business system's logical abstractions will be turned into physical systems that meet business objectives.[24] The six subcategories of questions at the physical layer are data assets (what), risk management practices (why), process mechanisms (how), human interface (who), infrastructure (where), processing schedule (when).[25]

F. *SABSA Component Architecture:*

Component architecture is the tradesman's view of the specialized components of the information system.[26] The information system will need a series of products and services from specialized vendors to complete the build, and people with the skills necessary to integrate the components to meet business objectives.[27] The six subcategories of questions at the component layer are assets (what), risk management components and standards (why), process components and standards (how), human entities: components and standards (who), locator components and standards (where), and step timing and sequencing components and standards (when).[28]

G. *SABSA Management Architecture:*

Management architecture is the service manager's view of how the information system must be operated, maintained, and monitored to ensure the system meets business requirements.[29] The management layer is unique because it must be integrated into the other five layers to facilitate the information system's proper operation.[30] The six subcategories of questions at the management layer are delivery and continuity management (what), operational risk management (why), process delivery management (how), governance, relationship and personnel management (who), environment management (where), time and performance management (when).[31]

H. *Additional SABSA Views*

Inspector's view and the governor's view are not recognized as separate views in the SABSA methodology because the framework as a whole provides the necessary support to achieve the objectives of the two remaining SABSA views.[32] The inspector's view audits the system and ensures that the "architecture is complete, consistent, robust and 'fit-for-purpose' in every way."[33]

---

[22] JOHN SHERWOOD ET AL., *supra* note 12, at 38.
[23] SABSA MATRICES 2018, *supra* note 1, at 7.
[24] SABSA WHITE PAPER, *supra* note 8, at 12.
[25] SABSA MATRICES 2018, *supra* note 1, at 7.
[26] SABSA WHITE PAPER, *supra* note 8, at 13.
[27] *Id*.
[28] SABSA MATRICES 2018, *supra* note 1, at 7.
[29] SABSA WHITE PAPER, *supra* note 8, at 13.
[30] *Id*. at 14.
[31] SABSA MATRICES 2018, *supra* note 1, at 7.
[32] SABSA WHITE PAPER, *supra* note 8, at 14-15.
[33] SABSA WHITE PAPER, *supra* note 8, at 14.

The governor's view governs the information system and encompasses the people (who) and motivation (why) columns in the SABSA matrix.[34] The governor's and inspector's views are essential to creating and maintain an effective compliance program in an interoperable, integrated clinical environment. The SABSA architecture can be combined with recently updated NIST materials to control and manage risk effectively throughout a health care enterprise.

NIST RESOURCE MATERIALS

Since the release of Version 1.0 of the Privacy Framework[35] in January 2020, the NIST created materials to assist professionals in integrating privacy, security, and enterprise risk management. One of the first supplemental materials released was a crosswalk between the NIST Privacy Framework and the Cybersecurity Framework.[36] The crosswalk links the cores, categories, and subcategories of the frameworks and facilitates the high-level integration of privacy and cybersecurity disciplines.

On 23 September 2020, the NIST released revision 5 of Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53 Rev. 5).[37] Upon the release of SP 800-53 Rev. 5, NIST noted that one of the most significant changes to the publication was that "[i]nformation security and privacy controls [were] now integrated into a seamless, consolidated control catalog for information systems and organizations."[38] The supplemental material provided with SP 800-53 Rev. 5 includes a mapping between the controls described in 800-53 and the NIST Cybersecurity and Privacy Frameworks.[39] Additionally, NIST provided a *Security and Privacy Control Collaboration Index Template* to facilitate collaboration between the security and privacy profession within an organization and ensure objectives are being met while the risk is managed.[40] NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations*, was released as a separate part of SP 800-53 Rev. 5 to help organizations establish a starting point for control selections to protect privacy and security

[34] *Id.* at 15.

[35] NIST PRIVACY FRAMEWORK, *supra* note 19.

[36] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., PRIVACY FRAMEWORK, CYBERSECURITY FRAMEWORK CROSSWALK (Jan. 16, 2020), https://github.com/usnistgov/PrivacyFrmwkResources/raw/master/resources/Cybersecurity%20Framework%20Crosswalk/Crosswalk%20Resource-%20Cybersecurity%20Framework%20to%20NIST%20Privacy%20Framework.xlsx.

[37] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUB. 800-53 REV. 5, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (Sept. 23, 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[38] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUTER SECURITY RESOURCE CENTER, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS: NIST PUBLISHES SP 800-53, REVISION 5 (Sept. 23, 2020), https://csrc.nist.gov/News/2020/sp-800-53-revision-5-published.

[39] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUTER SECURITY RESOURCE CENTER, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS, SUPPLEMENTAL MATERIAL, MAPPINGS: CYBERSECURITY FRAMEWORK AND PRIVACY FRAMEWORK TO REV. 5 (updated Jan. 22, 2021), https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx.

[40] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUTER SECURITY RESOURCE CENTER, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS, SUPPLEMENTAL MATERIAL, CONTROL COLLABORATION INDEX TEMPLATE (updated Dec. 10, 2020), https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53-collaboration-index-template.xlsx.

of information systems.[41] Creating a starting point for controls is essential to an enterprise risk management strategy. The enterprise risk management strategy provides the foundations for an effective compliance program.

COMPLIANCE OUTCOMES NECESSARY FOR INTEGRATION

The use and transfer of ePHI are necessary to achieve the integrated clinical environment's goal; therefore, the information system upon which integration and interoperability occur must be developed to achieve compliance outcomes necessary in the health care environment.[42] The system's architecture must enable the seven elements of an effective compliance program.[43] HHS OIC Health Care Fraud Prevention and Enforcement Action Team (HEAT) defines the seven elements:

> 1. Implementing written policies, procedures, and standards of conduct.
>
> 2. Designating a compliance officer and compliance committee.
>
> 3. Conducting effective training and education.
>
> 4. Developing effective lines of communication.
>
> 5. Conducting internal monitoring and auditing.
>
> 6. Enforcing standards through well-publicized disciplinary guidelines.
>
> 7. Responding promptly to detected offenses and undertaking corrective action.[44]

NIST provides two complementary frameworks that address cybersecurity and privacy concerns and identify the necessary outcome for an effective program.[45] The CSF identifies five core functions: identify, protect, detect, respond, and recover.[46] The NIST Privacy Framework contains five core functions. The privacy framework's core functions are identify, govern, control, communicate, and protect.[47] The two frameworks, in addition to the NIST Risk Management Framework[48], enable organizations to develop effective policies, procedures, and standard operating procedures to address privacy and security risk in an integrated manner. The use of the

---

[41] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUB. 800-53B, CONTROL BASELINES FOR INFORMATION SYSTEMS AND ORGANIZATIONS 1 (updated Dec. 10, 2020), https://doi.org/10.6028/NIST.SP.800-53B.

[42] *See generally* W. Nicholson Price II, *Risk and Resilience in Health Data Infrastructure*, 16 COLO. TECH. L.J. 65 (2017); U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTH INDUSTRY CYBERSECURITY PRACTICES: MANAGING THREATS AND PROTECTING PATIENTS, PUBLIC HEALTH EMERGENCY (Jan. 4, 2019), https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx.

[43] DEP'T OF HEALTH & HUMAN SERVS, OFFICE OF INSPECTOR GEN., HEALTH CARE COMPLIANCE PROGRAM TIPS., https://oig.hhs.gov/compliance/provider-compliance-training/files/Compliance101tips508.pdf.

[44] *Id*.

[45] NIST PRIVACY FRAMEWORK, *supra* note 19; NIST CYBERSECURITY FRAMEWORK, *supra* note 18.

[46] *Id.* at 7 – 8.

[47] NIST PRIVACY FRAMEWORK, *supra* note 19, at 7.

[48] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUB. 800-37, REV. 2, RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS (Dec. 2018), https://doi.org/10.6028/NIST.SP.800-37r2.

SABSA methodology enables the development of an architecture that systematically integrates the cybersecurity and privacy disciplines while ensuring the implementation of an effective compliance program. The SABSA inspector, governor, and management views provide the architecture necessary to align the compliance program with business objectives. Compliance can be achieved if privacy and security are engineered into the interoperable health information systems through the SABSA methodology.

CHALLENGES FOR AN INTEROPERABLE, INTEGRATED CLINICAL ENVIRONMENT

An interoperable, integrated clinical environment presents unique challenges due to the fast-moving free-flow of ePHI. Data provenance is a record of the origin of data. The data input into interoperable systems will inform decisions about the originating patient and broader health care analytics. If the information is not accurate, the interoperable system must track the data path to correct the data in all locations where it resides. Additionally, patients permitting their data to enter into an interoperable system must know where their data has gone. Provenance is an essential element in generating trust in an interoperable health care system.

Patient matching is essential to the safety of interoperable health information technology systems. In 1996, HIPAA required the development and use of the unique patient identifier; however, due to security concerns, appropriations bills were passed preventing HHS from using any appropriated funds to develop a unique patient identifier.[49] Health information of a single patient is likely to travel through several different health care institutions that use different identifiers. The safety of a patient depends on clinicians being able to access accurate information on a patient quickly. The risk of inaccurate information could be mitigated by adopting a unique patient identifier for each patient's data that enters the interoperable system. Metadata such as demographics can be used for matching, but the matching algorithms are only as good as the data in the system. Patients may have the same names, dates of birth, and addresses, thereby preventing accurate matching. However, this problem could easily be solved by a unique identifier. Additionally, a unique identifier would allow a patient to determine where their data is located on the health information network by tracking the unique identifier. A unique patient identifier would address both privacy and safety concerns.

Metadata is data about data. It is the who, what, when, where, why, and how of data in a system. Metadata is closely linked to both provenance and patient matching. The interoperable health care information system must have sufficient information about the system's data to evaluate its accuracy and determine its relevance to other data points in the system. The interoperable, integrated clinical environment will heavily depend on metadata to exercise appropriate security and privacy controls; therefore, the information systems must be engineered to contain the necessary metadata to ensure accuracy and maintain privacy as the data moves throughout the system.

HIPAA Notice of Privacy Practices is the tool that covered entities use to obtain authorization to use and disclose patient data. However, common notices of privacy practices are

[49] Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-facilitated Exchanges and Health Care Providers, 84 Fed. Reg. at 7614-15.

likely to provide insufficient notice of how a patient's data could be used in an interoperable health information system. Health care organizations must first understand how data will be processed throughout the health information system to obtain proper authorization. Knowledge is key to obtaining authorization and developing trust. Creating the architecture of an interoperable, integrated clinical environment should also drive the development of more effective notices of privacy practices.

Permission is closely related to patient authorization and notices of privacy practices. Health care organizations will not have permission to process data in an interoperable system unless proper authorization is obtained. The system must be engineered to ensure a patient's authorization automatically creates the appropriate permissions in the system and that those permissions are enforced as the data moves throughout the interoperable system. If permissions are not enforced, then the authorization becomes meaningless and could easily foster an atmosphere of distrust in the health care system.

Big-data, re-identification, and anonymization represent a significant challenge to the interoperable health information system described by ONC Health IT. The areas of population health and research would gain the most from analyzing large data sets. Additionally, the use of consumer electronics to gather health data on individuals suggest that ePHI will be distributed to large organizations that aggerate, analyze, and monetize data. The use of ePHI by giant data aggregators represents a significant risk to patient privacy. Additionally, the interoperable health information system must be capable of disassociability of individual identity to enable the data minimization principle when processing data for population health and research.

CONCLUSION:

An interoperable, integrated clinical environment can be private and secure if the SABSA methodology is used to integrate the NIST frameworks during the design, development, deployment, and maintenance of health information systems supporting integration and interoperability; however, the interoperability of the systems and exchange of health data between the integrated clinical environment introduces another layer of complexity to evaluating and mitigating privacy and security risks. If the risks are not systematically addressed throughout the enterprise and systems lifecycle, the goals of the integrated clinical environment cannot be achieved. Privacy and security must be engineered into healthcare information systems.

Privacy engineering is the act of building the architecture. The NIST Privacy Risk Analysis Methodology[50] informs the risk assessment. The NIST Risk Management Framework[51] prepares and informs the enterprise of proper risk management practices. The NIST CSF[52] and Privacy Frameworks[53] identify essential organizational functions necessary to protect privacy and security.

[50] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[51] NIST RISK MANAGEMENT FRAMEWORK, *supra* note 48.

[52] NIST CYBERSECURITY FRAMEWORK, *supra* note 18.

[53] NIST PRIVACY FRAMEWORK, *supra* note 19.

The SABSA[54] methodology provides the architecture to integrate the frameworks and engineer a private and secure interoperable, integrated clinical environment.

Frameworks and methodologies exist to enable health care organizations to design information systems that protect patient privacy and security while achieving enterprise business goals. Healthcare organizations must create and maintain information systems that are designed to protect privacy and security through appropriate enterprise risk management practices. Additionally, privacy and security officers must become an integral part of the risk management, compliance, contracting, and acquisition processes of healthcare organizations to ensure ePHI remains both private and secure throughout the information systems lifecycle. The goal of the health care enterprise must be to prove to patients that an integrated and interoperable health care delivery system will protect the privacy and security of their health information while improving their health.

[54] SABSA WHITE PAPER, *supra* note 8.