JOURNAL OF
HEALTH
CARE
FINANCE

Fall 2019

SECURITY AND PRIVACY OF THE INTEGRATED CLINICAL ENVIRONMENT PART I

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

INTRODUCTION

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

The integrated clinical environment is the synthesis of health care providers, medical devices, health information networks and information technology working together to improve patient safety, increase treatment effectiveness, and improve efficiency. Although this is a laudable goal, current research has done little to address security and privacy concerns with the integrated clinical environment. Unfortunately, the concept was born with little focus on security and privacy. The potential for great harm, both physical and emotional, is ever-present in the health care context when information technology is used to assist in the treatment of patients. The basic tenants of information security should be followed when developing an integrated clinical environment—confidentiality, integrity, accessibility, and accountability.

Additionally, privacy concerns outlined in the Fair Information Practice Principles—access and amendment, accountability, authority, minimization, quality and integrity, individual participation, purpose specification and use limitation, security, and transparency—must also be addressed when creating an integrated clinical environment. Integration without security and privacy is not interoperability. A health care organization cannot operate an integrated clinical environment in today's legal and regulatory environment without assurances of security and privacy engineered into the systems. However, frameworks currently exist that enable health care organizations to manage both security and privacy risk throughout the enterprise systematically.

Security and Privacy of the Integrated Clinical Environment will be presented in a series of three articles. The first article, Part I, discusses 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 associated with the deployment of an interoperable ICE. The second article, Part II, will discuss 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. Finally, the third article, Part III, will discuss how the Sherwood Applied Business Security Architecture (SABSA) can be used to integrate the frameworks and methodologies presented in Part II into an enterprise architecture to ensure an organization deploying an interoperable, ICE is compliant with their obligation to protect the privacy and security of a patient's health information.

INTEGRATED CLINICAL ENVIRONMENT

A. *ASTM F276109(2013)*

ASTM International (ASTM) began in 1898 as the American Society for Testing and Material and has developed over 12,000 voluntary consensus standards to improve quality, enhance health and safety, and build consumer confidence.[1] ASTM works with top experts and business professionals throughout the world openly and transparently to develop test methods, specifications, classifications, guides, and practices that support the needs of governments and

[1] *Detailed Overview*, ASTM INTERNATIONAL (last accessed Apr. 7, 2019), *https://www.astm.org/ABOUT/full_overview.html.*

industries worldwide.[2] The integrated clinical environment (ICE), as defined by ASTM, is an "environment that combines interoperable heterogeneous medical devices and other equipment integrated to create a medical system for the care of a single high acuity patient."[3] The goals of ICE are to "improve patient safety, treatment efficiency, and workflow efficiency than can be achieved with independently used medical devices."[4] The environment centers around the care of one patient and can include data acquisition, safety interlocks, system integration, and distributed closed-loop control. The fundamental concept of the ICE is that the components of the system function interdependently as a single system and not as independent medical devices. Additionally, the ICE, as described by ASTM F276109(2013), is composed of devices from several different manufacturers that are not manufactured to operate in conjunction with devices from other manufacturers.[5] When evaluating ICE for compliance purposes, close attention must be paid to the fact that the ICE is intended to operate interdependently. The intended interdependence raises compliance and legal issues that must be addressed to ensure ICE is compliant when utilized in a clinical environment. The ICE is patient-centric and should move with the patient as she moves through different health care settings.[6]

The integrated clinical environment utilizes several terms that must be understood in the appropriate context to appreciate the challenges to privacy and security inherent in an ICE implementation. ASTM F276109(2013) defines several important ICE components.

Patient: living being (person or animal) undergoing a medical, surgical, or dental procedure.[7]

Medical Device: any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purposes(s) of diagnosis, prevention, monitoring, treatment or alleviation of disease, diagnosis, monitoring, treatment, alleviation of or compensation for an injury, investigation, replacement, modification, or support of the anatomy or of a physiological process, supporting or sustaining life, control of conception, disinfection of medical devices, providing information for medical purposes by means of in vitro examination of specimens derived from the human body, and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which can be assisted in its function by such means.[8]

ICE Equipment Interface: part of ICE compatible equipment that provides the interface to the ICE network controller.[9]

Device Model: representation of the capabilities of ICE compatible equipment that includes the information needed to qualitatively and quantitatively describe, control, and monitor its operation.[10]

[2] *Id.*

[3] ASTM INTERNATIONAL, F2761-09 (2013) MEDICAL DEVICES AND MEDICAL SYSTEMS - ESSENTIAL SAFETY REQUIREMENTS FOR EQUIPMENT COMPRISING THE PATIENT-CENTRIC INTEGRATED CLINICAL ENVIRONMENT (ICE) - PART 1: GENERAL REQUIREMENTS AND CONCEPTUAL MODEL 3 (2013).

[4] ASTM INTERNATIONAL, *supra note 3*, at 1.

[5] ASTM INTERNATIONAL, *supra note 3*, at 3.

[6] ASTM INTERNATIONAL, *supra note 3*, at 14.

[7] ASTM INTERNATIONAL, *supra note 3*, at 4.

[8] ASTM INTERNATIONAL, *supra note 3*, at 4.

[9] ASTM INTERNATIONAL, *supra note 3*, at 4.

[10] ASTM INTERNATIONAL, *supra note 3*, at 2.

ICE Network Controller: part of the ICE that provides communication between ICE compatible equipment and the rest of ICE, using the device model.[11]

ICE Supervisor: part of an ICE that provides a platform for functional integration between ICE compatible equipment via the ICE network controller and can provide application logic and an operator interface. *Application logic to include clinical algorithms, distributed control integration, and clinical decision support algorithms*.[12]

ICE Manager: the ICE network controller and the ICE supervisor, these components can be integrated.[13]

Operator: the person handling the equipment.[14]

External Interface: permits communication between the ICE network controller and an external network.[15]

[11] ASTM INTERNATIONAL, *supra note 3*, at 3.

[12] ASTM INTERNATIONAL, *supra note 3*, at 3. The ICE supervisor is where clinical decision support would reside within an ICE implementation. The algorithms utilized for clinical decision support can be generated by data received from an interoperable health information system.

[13] ASTM INTERNATIONAL, *supra note 3*, at 8. The ICE external interface connects the patient-focused ICE with the broader health information system. The external interface is where interoperability begins.

[14] ASTM INTERNATIONAL, *supra note 3*, at 4.

[15] ASTM INTERNATIONAL, *supra note 3*, at 8.

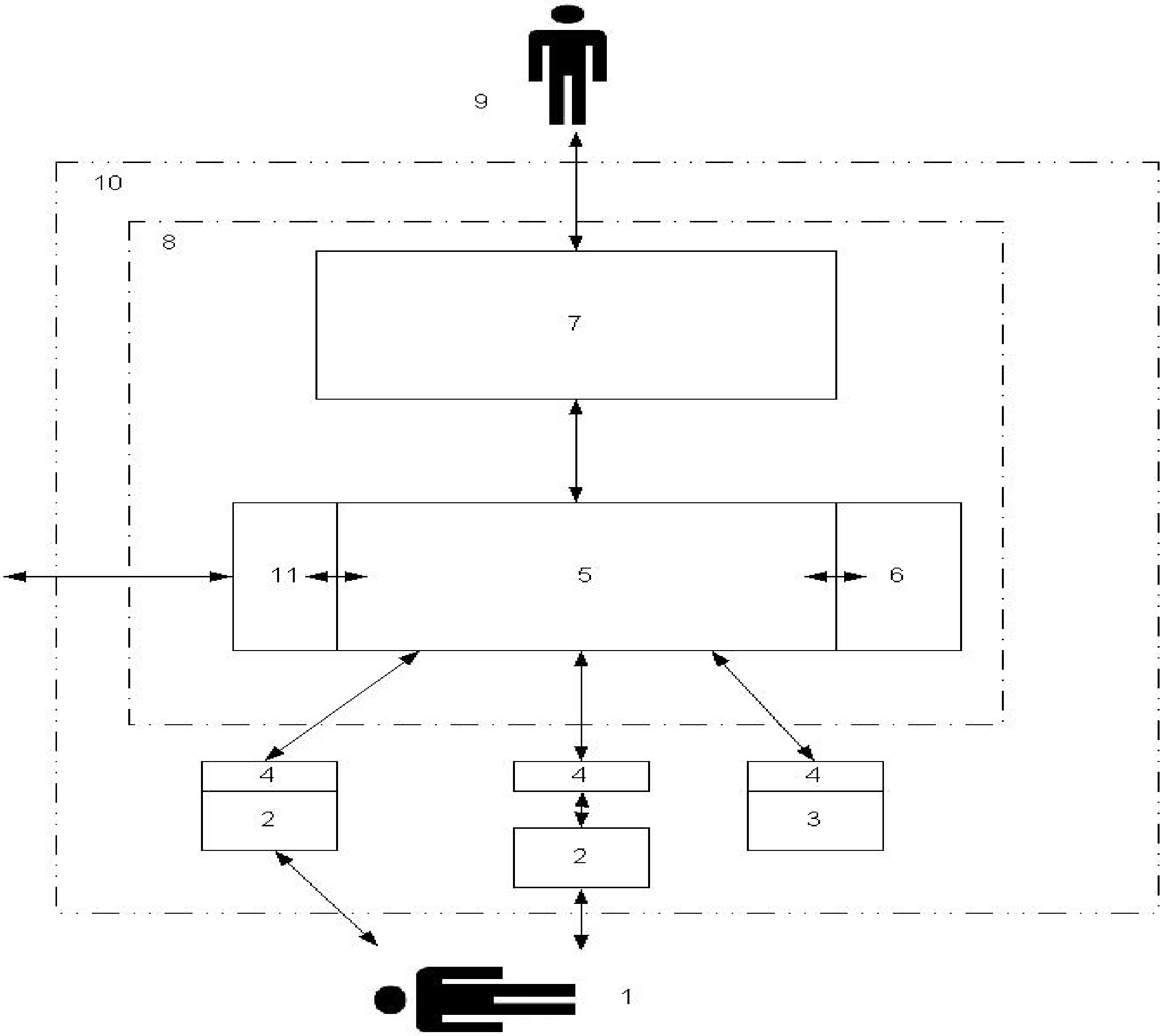

Figure 1. Conceptual Model of the ICE.[16]

Legend: (1) Patient; (2) Medical Device; (3) Equipment; (4) ICE Equipment Interface; (5) ICE Network Controller; (6) Data Logger; (7) ICE Supervisor; (8) ICE Manager; (9) Operator; (10) ICE; an (11) External Interface.

The ICE network controller is responsible for ensuring that the functional capabilities of the medical devices attached to the network are delivered reliably to the ICE supervisor. If the functions cannot be delivered reliably, the ICE network controller must generate and sound an alarm. The ICE network controller is also responsible for providing the association and communication with each ICE equipment interface. The ICE network controller interface is another critical concept in the ASTM model. The ICE network controller interface is a port on the network controller that provides communication with an ICE equipment interface and covers the first four layers in the ISO reference model.[17] The first four layers being physical, data link, network, and transport. The ASTM states that a "key objective is to make the implementation of the upper layer of the communication stack of the ICE network controller independent of the

[16] ASTM INTERNATIONAL, *supra note 3*, at 6.
[17] ASTM INTERNATIONAL, *supra note 3*, at 7.

particular ICE equipment interface."[18] The ICE network controller must also support a connection to the ICE Supervisor. The ICE network controller connects to an external interface, such as a hospital's information system.[19] Finally, the ICE network controller must have forensic data logging capabilities that allow a timestamped state for the clinical environment.

The ICE supervisor is responsible for ensuring functional capabilities, and nonfunctional requirements are suitable for the intended use of the ICE supervisor. If they are not suitable, then the supervisor should sound an alarm.[20]

The ASTM states that the benefits of ICE are clinical decision support; automated workflow support; medical device safety interlocks; reduction of use errors; distributed physiologic closed-loop control of e.g., medication, fluid delivery, anesthetic agent delivery, and ventilation; monitoring of medical device activity and performance; automated system readiness assessment (e.g., prior to starting invasive clinical procedures); support of remote monitoring of the intensive care unit; safeguarding of protected patient information through real-time encryption; seamless connection and disconnection ("plug-and-play") of medical devices without shutting down and rebooting the medical devices or the ice network controller ("hot-swapping"); facilitation of disaster preparedness: real-time inventory of equipment in use and in strategic national stockpiles, and rapid deployment of medical devices in makeshift emergency care settings; avoidance of unnecessary redundancy by using shared resources, e.g. one connection to the electronic medical record system (EMRS); reduction of the cost and implementation barriers to technology-dependent innovation.[21]

The ASTM F276109(2013) is part one of a five-part series. The first part only addressed the general requirements of ICE and the conceptual model. This standard does not address security. The standard was not expected to address the requirement for safe and reliable integration until part five in the series. The late introduction of security into the ASTM conceptual ICE model fails to address a primary business concern of health care entities—compliance. The key concept here is that the ASTM did not address security concerns adequately when conceptualizing ICE. The word "security" can only be found twice in the standard.

B. *Clinical Applications of ICE*

Patient-controlled analgesia (PCA) pumps are commonly used in the postoperative clinical environment to control pain. The intravenous analgesic commonly used can cause a patient's respiratory rate to drop to a dangerously low level, respiratory compromise, resulting in severe injury or death. The delayed detection of respiratory compromise is not uncommon in the clinical setting due to alarms excessively sounding because the alarms are not specific to each patient. The ICE solution to this issue would be to integrate a PCA pump, pulse oximeter, and respiratory rate monitor into a system that would automatically stop the PCA pump if the patient's physiological parameters move outside a predetermined range.[22]

In another application of ICE to a PCA pump case, the patient is connected to a PCA pump, a large volume infuser pump, a pulse oximeter, a blood pressure device, a respiratory rate monitory, and a distributed alarm system. Before the administration of any opioid through the PCA pump, the system would query the hospital information system for the patient's age, weight,

[18] ASTM INTERNATIONAL, *supra note 3*, at 7.
[19] ASTM INTERNATIONAL, *supra note 3*, at 8.
[20] ASTM INTERNATIONAL, *supra note 3*, at 9.
[21] ASTM INTERNATIONAL, *supra note 3*, at 13.
[22] ASTM INTERNATIONAL, *supra note 3*, at 22.

medication list, and contraindicating diagnosis. The system would then compare the physician's medication order with the values programmed into the PCA pump to determine the proper setup. The system would continually monitor the patient's physiological status and use an algorithm based on the patients' medical record to assess the state of the patient while attached to the PCA pump. If the algorithm detects the patient is in distress, then the PCA pump would be stopped, and an alarm sent to clinical personnel. If the systems detect the patient is in severe distress, a high priority alarm would be distributed to clinical staff.[23] Both examples of the PCA pump show that the concept of ICE would be implemented using algorithms to assist clinicians

The ICE can also help in clinical decision support for a hospital's rapid response team (RRT). The RRT is used to bring critical care expertise quickly to a patient's bedside. Patients usually exhibit abnormal vital signs hours before cardiorespiratory arrest; however, the RRT must sift through all available information when arriving at the bedside before determining the appropriate intervention. In an ICE implementation, a predetermined assessment is entered into the patient's record upon arrival to a noncritical unit. The system then collects physiological measures from the integrated medical devices, and clinical assessments from the staff are processed by an algorithm to determine if the patient's status is deteriorating and the RRT is alerted. Upon arrival at the patient's bedside, the RRT is presented with relevant data on the patient. The ICE system can go as far as presenting differential diagnoses, treatment algorithms, and checklists.[24] The RRT conceptualization of ICE is moving closer to making a diagnosis of an acute condition in a patient. As medical decisions using the ICE become more automated or guided by contextually generated checklists, the need for security within the ICE implementation becomes even more critical.

C. *Clinical Decision Support and Regulatory Issues of ICE Implementation*

The integrated clinical environment provides an excellent opportunity to improve clinical outcomes; however, the execution of an integrated clinical environment creates unique legal and regulatory issues. The ICE example provided above regarding the hospital's rapid response team is an example of clinical decision support (CDS). CDS is a computer program and the associated data that assist patients and health care practitioners in making clinical decisions.[25] However, the unique legal and regulatory issues created by the ICE systems must be identified.[26] CDS systems that recommend treatments based on algorithms that are beyond human comprehension could be characterized as practicing medicine.[27] However, the FDA has limited oversight of CDS systems.[28] Additionally, extensive FDA oversight of CDS systems that provides guidance on a significant number of ailments is likely to be impracticable if not impossible, given the amount of data that a CDS would need to be collected and assessed for each function of the system.[29] Interestingly, the focus on CDS systems is on clinical performance, safety, and effectiveness, not security and privacy.[30] The CDS systems collect and distribute vasts amounts of medical data that implicate patient privacy. Again, privacy has become a "bolt-on" element of the system or left entirely to

[23] ASTM INTERNATIONAL, *supra note 3*, at 22.

[24] ASTM INTERNATIONAL, *supra note 3*, at 26.

[25] Efthimios Parasidis, *Symposium: Clinical Decision Support: Elements Of A Sensible Legal Framework*, 20 J. HEALTH CARE L. & POL'Y 183, 186 (2018)

[26] *Id.*

[27] *Id.* at 191.

[28] *Id.*

[29] *Id.* at 208.

[30] *Id.*

another information system or appliance. The development of CDS systems appears to leave privacy and security as someone else's concern. However, the appropriate approach is to design security and privacy into the systems from inception.

Interoperable medical devices also create risks that must be properly classified to understand how risks in an ICE can be identified and mitigated.[31] The ICE presents a unique security challenge to medical devices due to network connections and coordinating functions between devices.[32] Security is essential because interoperable medical devices will be employed in settings where malfunctions or malicious attacks could create life-threatening situations.[33] The interconnection of the devices also introduces a new concern because only the weakest device in the ICE would need to be attacked to compromise privacy and security in the entire system.[34]

D. *ICE Attacks*

Attackers targeting ICE devices can be placed in two general categories: passive attackers who intercept traffic between devices and an active attacker who alter messages and compromise the integrity of the ICE.[35] Five classes of attacks have been identified:

> **Destroy**
>
> These attacks physically destroy some or all of the components in an interoperability environment, stopping its operation immediately. For example, an attacker could cut an infusion pump tube.
>
> **Disturb**
>
> These attacks modify the data available to some or all of the entities in the environment to prevent them from operating correctly. Examples include replay and man-in-the-middle attacks.
>
> **Reprogram**
>
> A particular subset of disturb attacks, these attacks modify data or code in a medical device, the coordinator, or the alarm system such that it doesn't perform its designated operation. For example, an attacker could modify an infusion pump's software to deliver extra medication. Reprogramming can be done locally or remotely if a device provides over-the-network programmability.
>
> **Denial of Service**
>
> These attacks target the network but also affect the devices, coordinator, or alarm system to prevent effective interoperation. For example, an attacker could burn out an infusion pump's motors through overuse, preventing the device from performing the required therapeutic functions.
>
> **Eavesdrop**
>
> These attacks involve listening in on the IMD environment's network to learn sensitive health information. Because these attacks (unlike the previous ones) don't disrupt system operation, detecting them is difficult.[36]

[31] Krishna K. Venkatasubramanian et al., *Security and Interoperable Medical Device Systems: Part 1.* IEEE SECURITY & PRIVACY 10(5), 61-63 (2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3797602/.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

When an ICE comes under attack, it can fail in two ways, fail-loud or fail quiet.[37] In a fail-loud scenario, the device sounds an alarm when it fails and alerts clinical personnel or the patient to the failure.[38] In a fail-quiet scenario, the device fails without sounding an alarm; for example, a monitoring device could broadcast unencrypted data on the network that is subject to eavesdropping by an attacker.[39] Failure states can be further categorized into different substates: fail-stop:fail-safe, fail-quiet:fail-stop, fail-quiet:fail-safe, fail-loud:fail-stop, fail-loud:fail-safe, and fail-loud:fail-quiet.[40] Each attack and the corresponding failure of an ICE device have corresponding consequences depending on the environment in which it is deployed.[41] The privacy and security implications can be significant; therefore, each ICE deployment must be evaluated to determine the actions necessary to mitigate risk to an acceptable level, the risk to both patient safety and privacy. The fail loud state produces clear benefits by alerting medical personnel or patients of the failure and mitigating the harmful effect. However, fail loud requires that the ICE will not survive if the alarm is destroyed and that the alarm cannot be reprogramed or disturbed.[42] ICE systems must be classified appropriately to understand the impacts of attackers and enable engineers to make informed decisions about ICE system design concerning safety and privacy.[43]

The security and privacy concerns of the ICE systems is further complicated by the commercialization of health data and consumer devices collecting and storing health data. Companies such as Amazon, Google, and Apple have recently signaled their desire to enter health care markets to access, store, and analyze patient data. HIPAA only applies to covered entities and not consumer-facing companies who collect and analyze data directly from consumers.

INTEROPERABILITY AND DATA LIQUIDITY

The integrated clinical environment, interoperability, and health information exchanges offer the opportunity to create data liquidity throughout the health care information ecosystem,

[37] Eugene Y. Vasserman et al., *Security and Interoperable Medical Device Systems: Part 2: Failures, Consequences and Classifications* IEEE SECURITY & PRIVACY 10(6), 60-73 (2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3797599/.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.* The authors provide examples of attack consequences and representative scenarios:

> *Scenario 1a* involves destroy or DoS attacks on the coordinator. The coordinator's inability to respond causes the alarm system to sound. Individual devices, unable to reach the coordinator, go offline, and might sound their internal alarms. *Scenario 1b* involves disturb or reprogram attack on the coordinator. The alarm system might eventually sound an alarm if it detects abnormal patient health indicators. *Scenario 1c* is an extension of 1b in which both the coordinator and alarm system are compromised. The alarm system should be designed so that attackers cannot silence it without attacking it directly. *Scenario 2a* involves destroy or DoS attack that causes one or more devices to stop abruptly. *Scenario 2b* is an extension of 2a in which one or more devices and the alarm system are compromised, leading to fail-quiet for the IMD. *Scenario 2c* involves disturb or reprogram attack, causing one or more devices to misbehave. The alarm system isn't attacked. *Scenario 2d* is an extension of 2c in which the alarm system is also compromised, leading to fail-quiet for the IMD. *Scenario 3a* involves a disturb attack on the network—for example, modifying the packets being sent or selectively dropping them. *Scenario 3b* involves eavesdrop attack on the network—for example, listening in on the communication between entities. *Scenario 4* is when the alarm system is compromised and fails completely or partially.

Id (emphasis added).

[42] *Id.*

[43] *Id.*

enabling patients to fully benefit from advances in technology that require the assimilation of data to drive outcomes. Interoperability will drive the efficient exchange of data.

A. *The Goal of Interoperability*

The goal of interoperability is to create a set of standards that allows entities throughout the health care industry to easily exchange information in a seamless, secure, and reliable format.[44] Section 4003 of the 21st Century Cures Act defines interoperability as "health IT that enables the secure exchange of electronic health information with, and use electronic health information from, other health IT without special effort on the part of the user, and allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law."[45] The 21st Century Cures Act states that the exchange of health information must be secure and that the information only used as authorized; therefore, the 21st Century Cures Act recognizes the goals of interoperability cannot be achieved without privacy and security.

In 2015, the Department of Health and Human Services, Office of the National Coordinator for Health IT, released its Shared Nationwide Interoperability Roadmap (Health IT Roadmap).[46] The Health IT Roadmap outlined the following principles for nationwide interoperability: focus on value, be person-centered, protect privacy and security in all aspects of interoperability and respect individual preferences, build a culture of electronic access and use, encourage innovation and competition, build upon existing health IT infrastructure, one size does not fit all, simplify, maintain modularity, and consider the current environment and support multiple levels of advancement.[47] The Health IT Roadmap recognized the need for "shared standards and expectations" for policy and technical components of interoperability that address privacy and security.[48] Although the Health IT Roadmap identifies key policies, technical components, and outcomes necessary to achieve interoperability, the roadmap does not identify what shared standards should be utilized. The roadmap provides the conceptual framework to build upon but does not provide sufficient guidance necessary to operationalize interoperable IT that secures data and protects patient privacy. Regarding privacy, the Health IT Roadmap discusses patient authorization and correct representation of permissions in the health IT environment but does not address how the information system should ensure ePHI is processed consistent with the authorization and permission. However, frameworks exist that enable the engineering of private and secure health IT systems.

B. *Data Liquidity*

Data liquidity is at the core of interoperability, allowing the exchange of information between various information systems in the health care ecosystems and enabling patients to access

[44] U.S. DEP'T. OF HEALTH & HUMAN SERVS., OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH IT, 2019 INTEROPERABILITY STANDARDS ADVISORY (Jan. 2019), https://www.healthit.gov/isa/sites/isa/files/inline-files/2019ISAReferenceEdition.pdf.

[45] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1165 (2016), https://www.govinfo.gov/content/pkg/PLAW-114publ255/pdf/PLAW-114publ255.pdf

[46] U.S. DEP'T. OF HEALTH & HUMAN SERVS., OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH IT, CONNECTING HEALTH AND CARE FOR THE NATION, A SHARED NATIONWIDE INTEROPERABILITY ROADMAP: THE JOURNEY TO BETTER HEALTH AND CARE (Oct. 6, 2015), https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf.

[47] *Id.* at xiv.

[48] *Id.* at xii.

their health data to aid in care readily.[49] Data liquidity can be achieved through the use of application program interfaces (APIs) that use a standard language to communicate information about a patient. Data liquidity will be required to scale interoperability to the national level. As data liquidity becomes more prevalent throughout the health care system, the challenges to privacy and security will only increase as more providers exchange patient information. However, data liquidity should assist in addressing privacy concerns as a patient's health information should become easier to identify and categorize as exchange becomes more standardized.

C. *Interoperability Challenges*

Interoperability provides avenues for numerous benefits to patients and public health; however, the increased connections and flows of data presents challenges to data security and patient privacy.[50] Privacy and security challenges cannot be ignored and must be addressed by engineering privacy and security into interoperable systems at the design phase. Data liquidity and interoperability also face regulatory and legal challenges; therefore, policymakers must face the difficult task of evaluating competing interests and formulating a policy that both protects patient privacy while enabling interoperability.[51] Interoperability and data liquidity also enable health information to quickly and easily flow outside the HIPAA protected areas.

The interoperability goal for 2020, as stated in the ONC's Health IT Roadmap Infographic:

> Connecting and expanding sets of users and data sources through the use of #mHealth and #wearables. Advances in the sharing and use of patient-generated health data lead to consumer empowerment, person-centered care, active individual health management, and greater information sharing with the public health community.[52]

[49] Paul K. Courtney, *Data Liquidity in Health Information Systems*, 17 CANCER JOURNAL 219, 219-21, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3186070/pdf/nihms308981.pdf; *see also* 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016), https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf.; Dov Greenbaum, *Direct Digital Engagement of Patients and Democratizing Health Care*, 32 SANTA CLARA COMPUTER & HIGH TECH. L.J. 93 (2015); Sharona Hoffman, *Citizen Science: The Law and Ethics of Public Access to Medical Big Data*, 30 BERKELEY TECH. L.J. 1741 (2015).

[50] Medicare and Medicaid Programs; 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. 7610 (proposed Mar. 4, 2019); *see* Ralph Artigliere et al., *Diagnosing and Treating Legal Ailments of the Electronic Health Record: Toward an Efficient and Trustworthy Process for Information Discovery and Release*, 18 SEDONA CONF. J. 209 (2017); Nicolas Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (2017).

[51] Nicolas Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 184-89 (2017).

[52] U.S. DEP'T. OF HEALTH & HUMAN SERVS., OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH IT, CONNECTING HEALTH AND CARE FOR THE NATION, A SHARED NATIONWIDE INTEROPERABILITY ROADMAP: THE JOURNEY TO BETTER HEALTH AND CARE INFOGRAPHIC: PDF VERSION (last reviewed Dec. 18, 2018), https://www.healthit.gov/sites/default/files/2017-08/shared_nationwide_interoperability_roadmap.pdf; *see generally*, U.S. DEP'T OF HEALTH & HUMAN SERVS., THE OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., SHARED NATIONWIDE INTEROPERABILITY ROADMAP: THE JOURNEY TO BETTER HEALTH AND CARE (last reviewed May 9, 2019), https://www.healthit.gov/sites/default/files/2017-08/shared_nationwide_interoperability_roadmap.pdf.

ONC's vision of interoperability includes the collection and sharing of health data generated from mobile health applications and wearable devices. Devices that fall outside the traditional HIPAA protected areas. Policymakers must revise laws and regulations to address contemporary technology and proactively address emerging threats as technology evolves.[53] Interoperability will create new security and privacy challenges that are unlikely to be fully identified until systems are implemented.[54] Therefore, the health care industry must engineer methods to identify and mitigate emerging risks into the system development lifecycle.[55]

The exchange of health information must be appropriately regulated to ensure that interoperability does not harm patient privacy while increasing access and control of health information.[56] The 21st Century Cures Act requires regulatory agencies to address interoperability.[57] In March 2019, the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC Health IT) released proposed rules to advance interoperability and support the access, exchange, and use of electronic health information.[58] The CMS proposed rules sought comment on whether the existing privacy and security standards were sufficient.[59] The ONC Health IT proposed rules were more technical than the CMS proposal.[60] One proposed change at the heart of privacy and security are the privacy and security attestations.[61] The attestations require health information technology developers to indicate whether or not their application encrypts authentication credentials and supports multifactor authentication.[62] The proposed rules do not require certified health IT to have these basic functions essential to maintaining privacy and security.[63] Developing the appropriate

[53] *See* Terry, *supra* note 51 at 205-07.

[54] See, Thomas Clifford, *Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?*, 12 NW. J. L. & SOC. POL'Y 45 (2016); Keith Hoffmann & Dave Titus, *In This Issue, Data Sharing and The Transformation of Veterans' Healthcare: Opportunities And Challenges In Interoperability*, 30 HEALTH LAWYER 30 (Feb. 2018); Nicolas Terry, *Symposium: Appification, AI, And Healthcare's New Iron Triangle*, 20 J. HEALTH CARE L. & POL'Y 118 (2018); and Scott Shackelford et al., *Securing the Internet of Healthcare*, 19 Minn. *J.L. Sci. & Tech.* 405 (2018).

[55] *See*, 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 [*hereinafter* NIST RISK MANAGEMENT FRAMEWORK].

[56] *See* Michael J. Saks, et al., *Granular Patient Control of Personal Health Information: Federal and State Law Considerations* 58 JURIMETRICS J. 411(2018); Lara Cartwright-Smith, et al., *Health Information Ownership: Legal Theories and Policy Implications*, 19 VAND. J. ENT. & TECH. L. 207 (2016); Oliver J. Kim, *Ebbs and Flows: Issues in Cross-Border Exchange and Regulation of Health Information*, 26 ANN. HEALTH L. 39 (2017).

[57] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).

[58] 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 7610; Office of the Nat'l Coordinator for Health Info. Tech., Dep't of Health & Human Serv., 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424 (proposed rule Mar. 4, 2019).

[59] 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 7635.

[60] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. at 7424.

[61] *Id.* at 7450.

[62] *Id.*

[63] *Id.*

regulations in the era of interoperability will be challenging, but regulations should adopt standards that are currently accepted throughout the IT industry.

CURRENT LEGAL AND REGULATORY REQUIREMENTS

The integrated clinical environment and data exchanges will consume ePHI; therefore, legal and regulatory requirements must be defined to ensure the interoperable, integrated clinical environment is engineered to meet privacy and security requirements.

A. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*

HIPAA creates the legal requirement that all covered entities and business associates must protect the privacy of ePHI.

1. HIPAA and What Does It Protect:

HIPAA is designed to protect the health information of patients as their information is processed throughout the health care ecosystem.[64] Generally, HIPAA only permits the disclosure of protected health information for treatment, payment, or health care operations reasons.[65] HIPAA regulates the privacy and security of an individual's electronic protected health information with what is commonly called the Security Rule. HIPAA defines protected health information (PHI) as individually identifiable health information transmitted or maintained by a covered entity or its business associate in any form or medium.[66] HIPAA considers health information as non-individually identifiable health information when the following information regarding the individual or her relatives, employers, or household members has been removed from the data: (A) Names; (B) All geographic subdivisions smaller than a State; (C) All elements of dates (except year) for dates directly related to an individual; and all ages over 89; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code.[67] The Security Rule is located at title 45 of the Code of Federal Regulations part 160 and subparts A and C of Part 164. Security and privacy are addressed explicitly in 45 CFR 164 subparts A and C. HIPAA compliance is mandatory for all covered entities and business associates.[68] Any health care provider that transmits health information in electronic format is required to comply with the HIPAA Security Rule. All health care institutions implementing an ICE or participating in an information exchange would be required to comply with HIPAA. Violating HIPAA can lead to significant civil penalties for health care organizations and onerous corrective action plans. The criminal penalties for HIPAA violations can be up to a $250,000 fine and ten years in jail, or both.[69] HHS Office of Civil Rights can also assess significant civil momentary penalties for each HIPAA violation.[70]

[64] 45 C.F.R. Part 160 (2019); 45 C.F.R. Part 164, Subpart A and E (2019).
[65] 45 C.F.R. § 164.502 (2019).
[66] 45 C.F.R. § 160.103 (2019).
[67] 45 C.F.R. § 164.514 (2019).
[68] 45 C.F.R. § 160.102(a) (2019).
[69] 42 U.S.C. § 1320d-6 (2019).
[70] 45 C.F.R. § 160.404 (2019).

The administrative regulations implementing HIPAA can be challenging to apply in a health care organization with a sophisticated information system. HIPAA provides a table that references the Security Standards announced in the Security Rule. The Appendix to the HIPAA Security Rule is reproduced in Table 1 below.

Standards	**Sections**	**Implementation Specifications (R)=Required, (A)=Addressable**
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Login Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)

Standards	**Sections**	**Implementation Specifications (R)=Required, (A)=Addressable**
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Reuse (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

Table 1. Appendix A to Subpart C of Part 164—Security Standards: Matrix.[71]

2. *OCR Enforcement Actions:*

HHS Office of Civil Rights (OCR) has enforcement authority over covered entities and business associates processing ePHI. The OCR uses its authority to obtain settlements and

[71] 45 C.F.R. Appendix A to Subpart C of Part 164 (2019).

implement corrective action plans when data in possession of covered entities and business associates are breached.

In June 2018, an administrative law judge rule ruled in favor of the OCR and required MD Anderson to pay $4,348,000 in civil monetary penalties for failing to encrypt patient data. The investigation by OCR revealed that MD Anderson lost ePHI for over 33,500 individuals through the theft of one unencrypted laptop and two USB thumb drives. Although MD Anderson recognized the need to encrypt electronic devices, it failed to do so during a nearly two-year period. The judge determined that the OCR was permitted to assess a penalty for each day on noncompliance with HIPAA and for each record that was breached.[72]

In December 2015, the University of Washington Medicine (UWM) entered into a resolution agreement and corrective action plan with OCR agreeing to pay $750,000 after an employee downloaded an email attachment containing malware that exposed ePHI of approximately 90,000 individuals. The OCR found that UWM had failed to implement policies and procedures to prevent, detect, contain, and correct security violations. Explicitly, the OCR director stated, “All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical records that fails to provide appropriate oversight and accountability for all parts of the enterprise.”[73] This enforcement action demonstrates the need to have policies and procedures that protect the entire enterprise, not just the systems containing the EMR.

In May 2014, the New York and Presbyterian Hospital and Columbia University agreed to a monetary settlement totaling $4,800,000 ePHI of 6,800 patients became accessible to internet search engines. The investigation determined that a physician who developed applications for both organizations deactivated a personally owned server that was attached to the network. Because the network lacked technical safeguards, ePHI became accessible to the internet when the server was deactivated. The organizations only learned of the breach after the partner of a former patient found ePHI on the internet. Again, the OCR found that the organizations had not made any efforts to ensure the server was secure or conduct a risk assessment of all systems accessing ePHI at the institutions.[74]

In February 2017, Memorial Healthcare System agreed to pay HHS $5,500,000 for a potential HIPAA violation affecting ePHI of 115,143 individuals. The OCR investigation determined that ePHI had been impermissibly accessed by employees and disclosed to physician office staff. The login credentials of a former employee of an affiliated physician’s office had been used daily for nearly a year without detection. The organization had access policies in place but no procedures to review and identify access to the systems. Additionally, OCR found that the organization failed to review network activity by the workforce. The OCR acting director stated, “organizations must implement audit controls and review audit logs regularly. As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to

[72] HHS PRESS OFFICE. JUDGE RULES IN FAVOR OF OCR AND REQUIRES A TEXAS CANCER CENTER TO PAY $4.3 MILLION IN PENALTIES FOR HIPAA VIOLATIONS *(*June 18, 2018), https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html

[73] HHS PRESS OFFICE, $750,000 HIPAA SETTLEMENT UNDERSCORES THE NEED FOR ORGANIZATION-WIDE RISK ANALYSIS (December 2015), http://wayback.archive-it.org/3926/20170127185458/https://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html.

[74] *HHS PRESS OFFICE, DATA BREACH RESULTS IN $4.8 MILLION HIPAA SETTLEMENTS* (May 7, 2014), https://wayback.archive-it.org/3926/20150618190123/http://www.hhs.gov/news/press/2014pres/05/20140507b.html

cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen."[75]

This sample of enforcement actions demonstrates that the OCR expects health care entities to take security and privacy seriously. The cause of the breaches ranges from failure to encrypt, inadequate network controls, failure to audit, and downloading malware. All of the breaches described above could have been prevented or mitigated by basic information security measures and proper management. HIPAA is instructive to health care entities, but it also poses a significant risk if a provider fails to comply. A health care entity that intends to utilize an ICE must evaluate how the integration will impact the overall security and privacy of their IT infrastructure. Interoperability is only one part; security and privacy are another.[76]

B. *Physician's Duty to Maintain Confidentiality:*

Health care providers have an ethical obligation to maintain the confidentiality of a patient's health information disclosed to them during treatment.[77] The American Medical Association issued an ethics opinion stating that physicians have an ethical responsibility to restrict unauthorized access to medical records, maintain the capability to audit access to the medical record, ensure data security and integrity in medical records, and implement policies and procedures regarding record retrieval, sharing, access, release, and disposition.[78]

C. *Tennessee Patient's Privacy Protection Act:*

HIPAA does not exclude states from implementing their legal regimes to protect patient privacy. States provide additional protection to patient privacy through statutes creating private rights of action, the involvement of the state's attorney general, and common law rights of privacy.[79] Tennessee recognizes an implied covenant of confidentiality between physician and patient. "Any time a doctor undertakes the treatment of a patient, and the consensual relationship of physician and patient is established, two jural obligations (of significance here) are simultaneously assumed by the doctor. Doctor and patient enter into a simple contract, the patient hoping that he will be cured and the doctor optimistically assuming that he will be compensated. As an implied condition of that contract, this Court is of the opinion that the doctor warrants that any confidential information gained through the relationship will not be released without the patient's permission... Consequently, when a doctor breaches his duty of secrecy, he is in violation of part of his obligations under the contract."[80] Therefore, a physician would be exposed to potential liability in a Tennessee court if she fails to take reasonable measures to protect a patient's privacy.

[75] HHS PRESS OFFICE, $5.5 MILLION HIPAA SETTLEMENT SHINES LIGHT ON THE IMPORTANCE OF AUDIT CONTROLS (February 16, 2017), https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html.

[76] As of 15 August 2019, the OCR is investigating 527 breaches that were reported in the last 24 months. The breaches under investigation affect 44,320,801 individuals. U.S. DEP'T OF HEALTH & HUMAN SERV., OFFICE FOR CIVIL RIGHTS, BREACH PORTAL: NOTICE TO THE SECRETARY OF HHS BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (last visited Aug. 15, 2019), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=4E491D8789D83B461A12B540DC9CD64D.

[77] AMERICAN MEDICAL ASSOCIATION, CONFIDENTIALITY & ELECTRONIC MEDICAL RECORDS CODE OF MEDICAL ETHICS OPINION 3.3.2., https://www.ama-assn.org/delivering-care/confidentiality-electronic-medical-records

[78] *Id.*

[79] TENN. CODE ANN. § 68-11-1502 (2019); TENN. CODE ANN. § 68-11-1503(c). (2019); TENN. CODE ANN. § 68-11-1503(e)(1) (2019); TENN. CODE ANN. § 68-11-1504 (2019).

[80] *Givens v. Mullikin ex rel. McElwaney*, 75 S.W.3d 383 (Tenn. 2002).

D. *FDA and Industry Guidance on Software as a Medical Device*

Software as a Medical Device (SaMD) is not well-developed within the FDA regulatory framework. The FDA defines SaMD as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[81] The Federal Food, Drug and Cosmetic Act requires the FDA to regulate all medical devices. The FDA classifies medical devices based on the controls necessary to ensure safety and effectiveness based on the risk the device poses to a patient. Medical devices are placed into one of three classes: Class I, Class II, and Class III. Regardless of their classification, all medical device manufacturers must register with the FDA, list the medical devices they market, manufacture their devices consistent with Good Manufacturing Practices, and label their devices consistent with FDA regulations.[82] The International Medical Device Regulators Forum (IMDRF) provides guidance on risk categorization[83] and quality management practices that map to the FDA requirements for SaMD.[84] Class I devices such as an elastic bandage are not subject to any special controls.[85] Class II devices are subject to additional controls determined after the FDA reviews the device.[86] An example of a Class II device would be an infusion pump.[87] When the FDA lacks sufficient information to determine the risks posed by a device, the FDA will classify the device as a Class III device and require premarket approval.[88]

The software utilized within the ICE to enable interoperability could be characterized as SaMD by the FDA. SaMD does not include the software that is an integral part of the operation of a medical device. Therefore, the software utilized by an ICE to enable interoperability, operate alarms, and assist in clinical decisions could be characterized as a medical device separate from the hardware medical devices connected to the ICE implementation. The critical concept of ICE is that the system components are interdependent. This interdependence is created by the software that brings the various component into an ICE.

The FDA provides a few examples of software that is SaMD and software that is not. Examples of SaMD include: a smartphone app that allows MRI images to be viewed; software that provides parameters that become the input for a different device; software operating on a general-purpose computer that is indented to provide information for a medical purpose; software that is connected to a hardware medical device but is not needed by the medical device for its intended purpose; and any software intended for a medical purpose that is running on a general-purpose

[81] U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN, *SOFTWARE AS A MEDICAL DEVICE (SAMD)*, (Nov. 19, 2018), https://www.fda.gov/MedicalDevices/DigitalHealth/SoftwareasaMedicalDevice/default.htm.

[82] U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., CTR. FOR DEVICES & RADIOLOGICAL HEALTH, INFORMATION SHEET GUIDANCE FOR IRBS, CLINICAL INVESTIGATORS, AND SPONSORS 2 (Jan. 2006), https://www.fda.gov/downloads/regulatoryinformation/guidances/ucm127067.pdf.

[83] INT'L MEDICAL DEVICE REGULATORS FORUM, "SOFTWARE AS A MEDICAL DEVICE": POSSIBLE FRAMEWORK FOR RISK CATEGORIZATION AND CORRESPONDING CONSIDERATIONS (Sep. 18, 2014), http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf#search="Software%20as%20a%20Medical%20Device%20Possible%20Framework%20for%20Risk%20Categorization%20and%20Corresponding%20Considerations".

[84] INT'L MEDICAL DEVICE REGULATORS FORUM, SOFTWARE AS A MEDICAL DEVICE (SAMD): APPLICATION OF QUALITY MANAGEMENT SYSTEM (October 2, 2015), http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-151002-samd-qms.pdf.

[85] U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., *supra* note 82, at 2.

[86] *Id.*

[87] *Id.*

[88] *Id.*

computer.[89] The fundamental concept is that the software must be intended to be used for a medical purpose, e.i., treatment or diagnosis of a medical condition. Examples of software that is not SaMD include: software that is embedded into a medical device or firmware; software that is necessary for a hardware medical device to perform its intended function; software that relies on data from a medical device but does not itself have a medical purpose, encryption software; software related to workflows in clinical environments such as registration and scheduling; software that only monitors the performance of hardware medical devices; and databases that provide the inputs for software as a medical device.[90] The examples provided by the FDA show that some components of the ICE implementation would not be considered SaMD, where others such as alarms, software compiling and displaying clinical information, and software that uses algorithms to assist in the treatment of a patient could be considered SaMD. This area of the law is not clearly defined and represents a risk for an early adopter of ICE and interoperable health information systems.

In December 2017, the Food and Drug Administration (FDA) issued guidance on the clinical evaluation of Software as a Medical Device (SaMD).[91] The FDA adopted guidance from the IMDRF on the clinical evaluation of SaMD.[92] The IMDRF describes SaMD as "software that utilizes an algorithm (logic, set of rules, or model) that operates on data input (digitized content) to produce an output that is intended for medical purposes as defined by the SaMD manufacturer."[93] The IMDRF states that the clinical evaluation of SaMD is a three-step process that includes valid clinical association, analytical validation, and clinical validation[94]. The validation is necessary because health care decision that relies on the output of SaMD can have a significant impact on patient safety[95]. As the use of technology in health care increases, the risk to patient safety also increases if risks to patient safety are not properly evaluated and controlled.

The clinical evaluation is a three-step process designed to assess the safety, effectiveness, and performance of the SaMD. First, SaMD must have a valid clinical association meaning that the output must have clinical significance in the intended health care situation.[96] Second, SaMD must process the input data in a manner that generates an accurate, reliable, and precise output, analytical validation.[97] In the context of an ICE, the input data will come for a variety of sources, increasing the risk that the output generated by the algorithm is not reliable or accurate. Therefore, the security of the entire ICE implementation and the interoperable system where health data is gathered is crucial for the proper function of any SaMD with ICE. Finally, SaMD must pass clinical validation in that the output of the algorithm has a meaningful and positive impact on the health

[89] *What are examples of Software as a Medical Device*, U.S. DEP'T OF HEALTH & HUMAN SERVS., U.S. FOOD & DRUG ADMIN. (Dec. 6, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/SoftwareasaMedicalDevice/ucm587924.htm.

[90] *Id.*

[91] U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., CTR. FOR DEVICES & RADIOLOGICAL HEALTH, SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION, GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMIN. STAFF (Dec. 8, 2017), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm524904.pdf.

[92] INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM, SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION (Sep. 21, 2017), http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-170921-samd-n41-clinical-evaluation_1.pdf.

[93] INT'L MEDICAL DEVICE REGULATORS FORUM, *supra* note 84, at 11.

[94] *Id.* at 4.

[95] *Id.* at 7.

[96] *Id.* at 9.

[97] *Id.*

of the individual involved.[98] Any implementation of ICE that includes an algorithm intended to assist with patient care should be evaluated against FDA and IMDRF guidance to ensure it is compliant. Due to the interdependence of any ICE implementation, the software cannot be evaluated in isolation and must be developed with the security and privacy risks of the enterprise in mind.

In January 2019, the FDA released version 1.0 of the Software Precertification Program (Pre-Cert).[99] Per-Cert is a voluntary program designed to allow assessment of the safety and effectiveness of software without preventing patient access to advances in software technologies.[100] The FDA recognized that the traditional regulatory approach to hardware-based medical devices is ill-suited to SaMD.[101] Software is developed using agile methods allowing developers to respond and modify the products based on real-world performance.[102] Because the threat environment contains sophisticated malicious actors who adapt quickly to security controls, the agility of software development is necessary to respond quickly to evolving security and privacy threats. A slow and stiffly regulatory approach would likely increase the risk to patients and allow threats to exploit vulnerabilities, while software developers seek FDA approval to update SaMD. The FDA describes its proposed regulatory approach to SaMD as "an agile regulatory paradigm . . . necessary to accommodate the faster rate of development and potential for innovation in software-based products."[103] The Pre-Cert program will rely heavily on the industry to demonstrate a "culture of quality and organizational excellence and a commitment to monitor product performance."[104] If the industry operates responsibly, the FDA's regulatory burden will be reduced while patients benefit from SaMD incorporated into the ICE.

The goal of the Pre-Cert program is to build stakeholder confidence that developers of SaMD participating in the program "have demonstrated capabilities to build, test, monitor, and proactively maintain and improve the safety, efficacy, performance, and security of their medical device software products, so that they meet or exceed existing FDA standards of safety and effectiveness."[105] The FDA intends to evaluate developers of SaMD on five Excellence Principles: Product Quality, Patient Safety, Clinical Responsibility, Cybersecurity Responsibility, Proactive Culture.[106] The concept of patient privacy is only mentioned twice in the document and only in the context of cybersecurity concerns. Most likely, the FDA has overlooked specific privacy concerns

[98] *Id.* at 10.

[99] U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., DEVELOPING A SOFTWARE PRECERTIFICATION PROGRAM: A WORKING MODEL V1.0 (Jan. 2019), https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/UCM629276.pdf.

[100] *Id.* at 6.

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.* at 7.

[106] *Id.* at 11. The FDA defined the Excellence Principles. Product Quality – Demonstration of excellence in the development, testing, and maintenance necessary to deliver SaMD products at the highest level of quality. Patient Safety – Demonstration of excellence in providing a safe patient experience and emphasizing patient safety as a critical factor in all decision- making processes. Clinical Responsibility – Demonstration of excellence in responsibly conducting a clinical evaluation and ensuring that patient-centric issues, including labeling and human factors, are appropriately addressed. Cybersecurity Responsibility – Demonstration of excellence in protecting cybersecurity and proactively addressing cybersecurity issues through active engagement with stakeholders and peers. Proactive Culture – Demonstration of excellence in a proactive approach to surveillance, assessment of user needs, and continuous learning. *Id.* However, the FDA only mentions the word "privacy" twice in the 58-page document.

believing that cybersecurity mechanisms will adequately protect patient privacy. If privacy is not engineered into software systems processing large volumes of ePHI, health care consumers are likely to become concerned about how their data is being used and processed as SaMD becomes more mainstream in the health care ecosystem. The FDA should seek to integrate privacy controls into the Excellence Principles to ensure privacy is engineered into SaMD.

E. *FDA Guidance on Cybersecurity of Deployed Medical Devices*

The Food and Drug Administration (FDA) has provided little guidance on the security of medical devices after they are approved and placed on the market. Although the FDA has on issued guidance on this issue, the possible implications of FDA regulations require any entity implementing an ICE to utilize a systematic framework to evaluate the risk to patient safety throughout the enterprise to ensure the ICE would be compliant with FDA regulations after is it deployed and throughout its lifecycle.[107] However, the FDA's treatment of SaMD and adoption of industry guidelines suggest that broad and less prescriptive regulatory guidance coupled with strong industry standards could promise continued innovation while privacy and security are maintained or even strengthened.

The Cost of Privacy and Security Breach

A. *The Cost of a Data Breach*

In July 2018, the Ponemon Institute a report of a global study analyzing the costs of data breaches that have occurred over the 12 months preceding the report.[108] The report listed several factors that impact the cost of a data breach: the unexpected loss of customers following a data breach, the size of the breach and the number of records stolen, the time it takes to identify and contain the breach, effective management of detection and escalation costs, and the management of post-breach costs.[109] The report found that data breaches are most costly in the United States, that hackers and criminal insiders cause the most data breaches (48%), and the loss of customers had significant financial consequences.[110]

The average organizational cost for a data breach in the United States was $7.91 million.[111] The report found that highly regulated industries, such as health care, have the highest costs associated with data breaches. The per capita cost for each record breached in the health care sector was $406.[112] The report found that the health care industry had the highest rate of customer churn, 6.7 percent, associated with a data breach. The average customer churn rate associated with a breach was 5.4 percent.[113] Additionally, the United States had the highest notification costs associated with breaches at $740,000.[114] Additionally, the lost business costs in the United States

[107] See George Horvath, *Trading Safety for Innovation and Access: An Empirical Evaluation of the FDA's Premarket Approval Process*, 2017 B.Y.U.L. REV. 991 (2017); Michael Woods, *Cardiac Defibrillators Need To Have A Bulletproof Vest: The National Security Risk Posed By The Lack Of Cybersecurity In Implantable Medical Devices*, 41 NOVA L. REV. 419 (2017); U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., *supra* note 82.

[108] *PONEMON INSTITUTE, 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW* (July 2018), https://www.ibm.com/security/data-breach.

[109] *Id.* at 7.

[110] *Id.* at 9-10.

[111] *Id.* at 15.

[112] *Id.* 18.

[113] *Id.* at 25.

[114] *Id.* at 27.

were very high at approximately $4.2 million.[115] However, the extensive use of encryption reduced the cost of a breach by $13 per record. The use of internet of things (IoT) devices increased the cost of a breach by $5.40 per record.[116]. The health care sector also had the highest mean time to contain, 100 days, and the second-highest meant time to identify at 255 days.[117]

Baker & Hostetler, LLP, released its fifth annual data security incident report in April 2019.[118] The report analyzed over 750 incidents during 2018 and found the top five causes for security incidents were phishing, network intrusion, inadvertent disclosure, lost or stolen devices or record, and system misconfiguration.[119] The health care industry was the top industry affected by security incidents, accounting for more than 25 percent of the reported incidents.[120] Employees were responsible for 55 percent of the incidents.[121] Health information was at risk in 33 percent of the incidents, a close second to social security numbers at 37 percent.[122] The report concludes with eight baseline recommendations: increase awareness, conduct risk assessments, implement basic security measures, improve detection capabilities, prepare to respond, address business continuity, address vendor risks, and mitigate the financial impact.[123]

The Ponemon Institute and Baker Hostetler reports demonstrate that health care information is at risk and must be protected. The cost of a data breach for a large health care organization will be high, and the introduction of the IoT devices, analogous to interoperable ICE devices, increase costs. Because an ICE implementation is comparable to an IoT device, health care organizations must carefully assess and mitigate the additional risks posed by the connected nature of an interoperable ICE implementation.

B. *The Cost of Medical Errors and Device Malfunctions*

In 2016, a study conducted by Dr. Makary and Dr. Daniel of John Hopkins University School of Medicine concluded that medical error was the third leading cause of death in the United States. The interoperability of medical devices and their respective access to the hospital information system provides another gateway for a malicious actor to access the network. Additionally, the connection between medical devices and the introduction of additional user interfaces permit additional opportunities for negligent internal actors to harm the hospital information system, the network, and PHI privacy and security.[124] An insecure interoperable health information system could lead to increased medical error.

[115] *Id.* at 29.

[116] *Id.* at 22.

[117] *Id.* at 35.

[118] BAKERHOSTETLER, 2019 MANAGING ENTERPRISE RISK IN A DIGITAL WORLD, PRIVACY, CYBERSECURITY, AND COMPLIANCE COLLIDE (Apr. 4, 2019), https://www.bakerlaw.com/press/bakerhostetlers-5th-annual-data-security-incident-response-report-highlights-collision-of-privacy-cybersecurity-and-compliance-details-efforts-to-minimize-risk.

[119] *Id.* at 1-2.

[120] *Id.* at 3.

[121] *Id.* at 7.

[122] *Id.* at 11.

[123] *Id.* at 16.

[124] Michael Daniel & Martin Makary, *Medical error—the third leading cause of death in the US*, BMJ 353 (May 3, 2016), https://www.bmj.com/content/353/bmj.i2139.; Jill Van Den Bos et al., *The $17.1 billion problem: the annual cost of measurable medical errors*, 30 HEALTH AFFAIRS 596, 596-60 (April 2011), https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2011.0084?url_ver=Z39.88-2003&rfr_id=ori%3Arid%3Acrossref.org&rfr_dat=cr_pub%3Dpubmed; *Givens v. Mullikin ex rel. McElwaney*, 75 S.W.3d 383 (Tenn., 2002); *Walker v. Medtronic, Inc.*, 670 F.3d 569 (4th Cir. 2012); *Kubicki v. Medtronic, Inc.*, 293 F. Supp. 3d 129 (D.D.C. 2018); *Duggan v. Medtronic, Inc.*, 840 F. Supp. 2d 466 (D. Mass. 2012); *Bentzley v.*

C. *The Harm of a Privacy Violation*

In February 2019, the National Institute of Standards and Technology (NIST) released its Privacy Risk Assessment Methodology (PRAM).[125] The NIST PRAM includes a Catalog of Problematic Data Actions and Problems to include five categories of problems.[126] A problem can be defined as the specific harm an individual could suffer if their data is subject to unauthorized use or disclosures. The problems defined by the NIST PRAM are:

> **Dignity Loss**: Includes embarrassment and emotional distress.
>
> **Discrimination:** Unfair or unethical differential treatment of individuals, whether singly or as a group arising from the processing of data.
>
> **Economic Loss:** Can include direct financial losses as the result of identity theft or the failure to receive fair value in a transaction.
>
> **Loss of Self Determination**
>
> - **Loss of Autonomy:** Includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement.
> - **Loss of Liberty:** Incomplete or inaccurate data can lead to improper exposure to arrest or detainment. Improper exposure or use of information can contribute to abuses of governmental power.
> - **Physical Harm:** Physical harm or death.
>
> **Loss of Trust:** The breach of implicit or explicit expectations or agreements about the processing of data. These breaches can diminish morale or leave individuals reluctant to engage in further transactions, potentially creating larger economic or civic consequences.[127]

The problems described above are challenging for an organization to internalize and assess; therefore, an organization is unlike to prioritize mitigating privacy risk if it does not engage guided risk management throughout the enterprise.

Medtronic, Inc., 827 F. Supp. 2d 443 (E.D. Pa. 2011); *Federal Jury In Chattanooga Awards $22.26 Million In Malpractice Case*, THE CHATTANOOGAN.COM (March 13, 2010), http://www.chattanoogan.com/2010/3/13/170988/Federal-Jury-In-Chattanooga-Awards.aspx

[125] 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 [*hereinafter* NIST PRIVACY RISK ASSESSMENT METHODOLOGY].

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

[127] *Id.*

CONCLUSION

In Security and Privacy of the Integrated Clinical Environment Part I, the basic concepts of the integrated clinical environment, the clinical applications of ICE, and possible ICE attacks and risks were introduced. Following the introduction of ICE, the ideas of interoperability and data liquidity were discussed to provide insight into the challenges faced when sharing health information across the health care industry. Next, the current legal and regulatory requirements of an ICE were discussed to provide context and an understanding of the complexity of the system. Finally, the cost of privacy and security breaches was reviewed to ensure an understanding of the risk to both the business and the individual patient. In Part II, the NIST frameworks and privacy engineering concepts will be introduced to show how privacy and security risks can be addressed throughout the healthcare enterprise. The recently released NIST Privacy Framework V1.0[128] will be discussed throughout Part II and Part III to demonstrate how privacy risk in the integrated clinical environment can be systematically managed.

[128] 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 (Jan. 16, 2020), https://www.nist.gov/document/nist-privacy-frameworkv10pdf.