

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



# Risk in Healthcare Information Technology: Creating a Standardized Risk Assessment Framework

*Suzanna Schmeelk*

## Abstract

Data breaches are occurring at an unprecedented rate. Between June 2019 and early October 2020, over 564 data breaches affected over 36.6 million patients as posted to the United States Federal government HITECH portal. These patients are at risk for having their identities stolen or sold on alternative marketplaces. Some healthcare entities are working to manage privacy and security risks to their operations, research, and patients. However, many have some procedures and policies in place, with few (if any) centrally managing all their infrastructure risks. For example, many healthcare organizations are not tracking or updating all the known and potential concerns and elements into a centralized repository following industry best practice timetables for auditing and insurance quantification. This chapter examines known and potential problems in healthcare information technology and discusses a new open source risk management standardized framework library to improve the coordination and communication of the aforementioned problematic management components. The healthcare industry would benefit from adopting such a standardized risk-centric framework.

**Keywords:** risk associated with computer communications, healthcare, data breaches, GDPR, HITECH, HIPAA, standardized risk library, risk management, patient information, identity theft, cybersecurity, laws, penetration test, risk assessments, insurance

## 1. Introduction

Across the globe, data security is becoming more regulated. For example, in the European Union, the General Data Protection Regulation (GDPR) protects its citizens [1]. In China, the Cybersecurity Law of 2017 was one of the first well known laws passed to protect the data and communications of its citizens [2]. In the United States of America, medical entities in the country's critical infrastructure are covered under Federal laws to protect patient information. Specifically, the Health Insurance Portability and Accountability Act (HIPAA) [3] and Health Information Technology for Economic and Clinical Health Act (HITECH) [4] are Federal-level regulations for covered entities that secure patient-protected health information (PHI). PHI covers a gamut of different identifiers and includes patient

names, birthdays, social security numbers, medical record numbers, license plate numbers, biometric data, among a few others. The digital form of PHI is electronic PHI or ePHI. In the United States, vendors and services which are not covered under HIPAA (perhaps because they do not bill patients for services rendered) are regulated by the Federal Trade Commission (FTC) and must self-report health data breaches to the FTC [5]. Furthermore, the European Commission officially ratified the final version of the GDPR to include notification from a breached supervisory authority to be made within 72 hours (or provide reasons for a delay) [1].

In the United States, both HIPAA-covered and non-covered entities may also be under other legal requirements, such as non-disclosure, confidentiality restrictions, or other security requirements, for other organizational, research, or employee data.

The management within covered groups has historically remained siloed intra-organization where different components of the organizational risk are being managed and decisions made by different units within the organizations without a standardized and well-connected systematic methodology. For example, the legal, audit, budget, health informatics, security, privacy, medical, and information systems teams may all be disjointly managed, causing frustrations in adequately quantifying and coordinating the organizational risks. In such disjoint cases, an exception to an organizational policy may result in unidentified operational risk if the different departments are not consistently coordinated and periodically reviewing, perhaps updating, the associated risks.

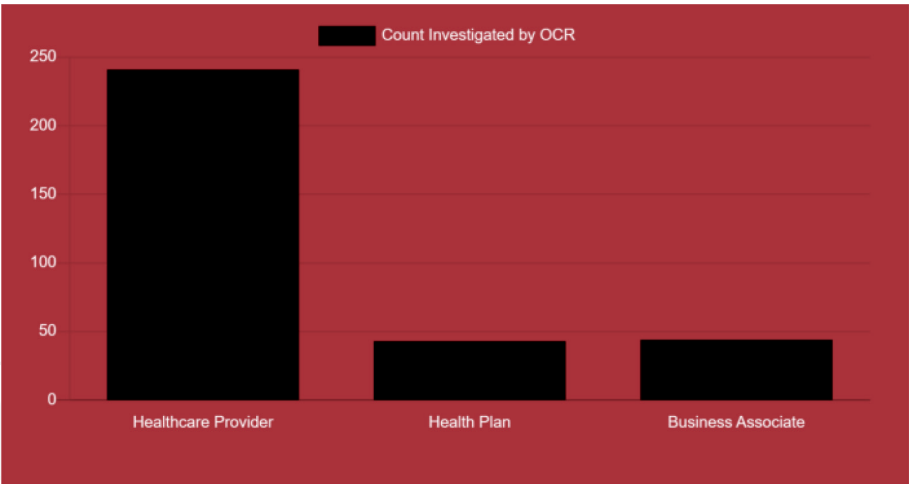
This chapter begins by describing data breach risks in HIPAA-covered entities as reported to the United States government that cause patients higher risks for identity theft. Then it integrates current research into building a standardized risk assessment library that enables both inter- and intra-organizational risk coordination. This design facilitates standardizing and communicating risks as well as reasonable internal statistics related to technical and administrative limitations, organizational policy exceptions, and federal legal requirements to inform the business, auditors, insurance companies, and business associates of risks.

## **2. Patient information data breaches can lead to patient identity theft**

In the United States, citizens are protected by federal, state, and potentially smaller sub-state regulations. Each industry sector are potentially under unique legal and other sector-specific requirements. In fact, today most, if not all, states have different personally identifying information (PII) legislation. Historically, these laws are not well understood and are written in most cases by non-technical writers. As such, the legal and technical specifications have gaps both in understanding and in the feasibility of current technological constraints.

### **2.1 Entities covered under HIPAA**

HIPAA requires at least three covered groups, referred to by the law as Covered Entities, to protect health information. Examples of covered entities are: healthcare providers, health Plans, and business associates. Healthcare providers transmit electronic patient information in connection with a Health and Human Services (HHS)-adopted standard transaction. Health plans include insurance companies, health maintenance organizations (HMOs), corporate health plans, and government programs. Business associates are external groups/organizations that perform activities or services on ePHI on behalf of another group covered



**Figure 1.**  
*OCR-covered entities investigated.*

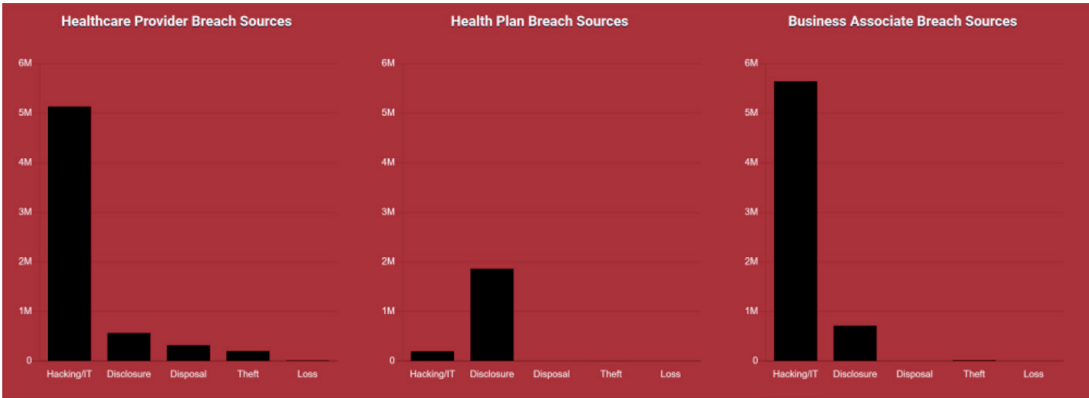
under HIPAA. **Figure 1** [6] shows one year of reports by covered entity to the Office of Civil Rights (OCR).

**2.2 Risks in HIPAA-covered entities**

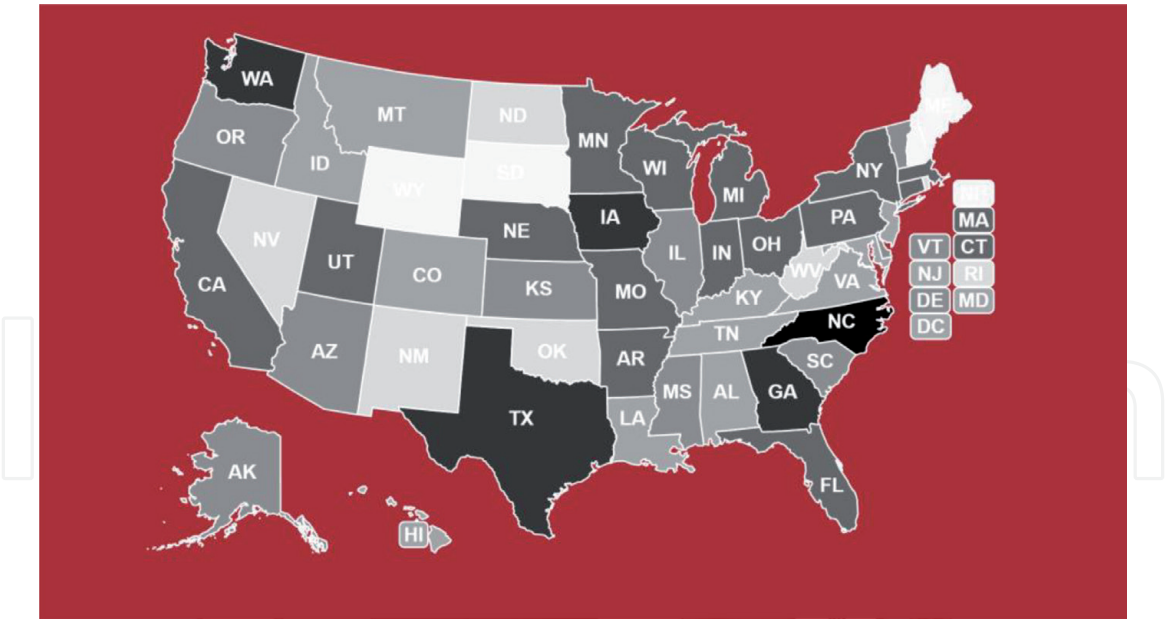
Research at large has studied risk management of medical information [7–10], but not specifically as related by different HIPAA-covered domains. Recent research [6, 7, 11] explores potential concerns for each legally covered segment based on self-report to the US Government as required by the HITECH Act. In the sector-specific threat probability-specific research [6, 7, 11] over a one-year interval, the research showed that different the different domains may indeed have different sources of concerns and issues. For example, healthcare providers and business associates have reportedly different higher probability of concerns to alleviate than health plan entities, as shown in **Figure 2** [6]. This indicates that the different domains may need to manage their threats differently by perhaps investing more heavily in different mitigating controls.

**2.3 Data breaches reported to the HHS OCR across the USA**

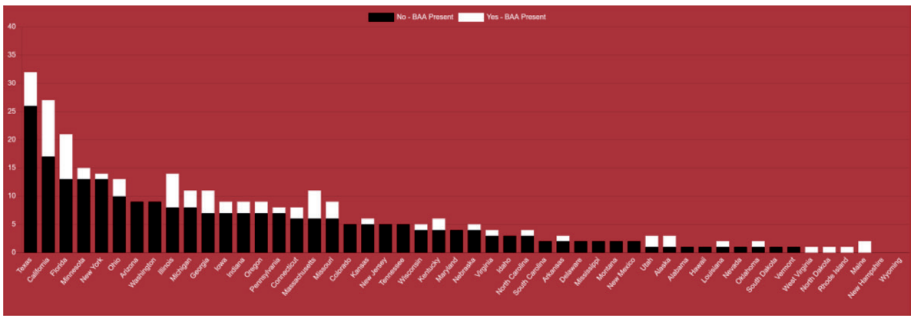
The HHS unauthorized data release portal provides the number of affected individuals from the cybersecurity events for each self-reported or discovered data release. **Figure 3** [6] shows states across the USA with the most reported individuals, whom are now at risk from the leaking of their patient data. In any given



**Figure 2.**  
*OCR-covered entities risk sources.*



**Figure 3.**  
*OCR breached individuals by state.*



**Figure 4.**  
*OCR-covered entities investigated BAA by state.*

one-year interval, each state may be equally likely to have higher counts depending on the released data size. Further research is needed to determine state likelihood.

2.4 Reported data breach counts per state sorted by number of reports

Another element tracked on the HHS portal is the presence of business associate agreements (BAA). A provider enters into a BAA with an outside party when an outside party receives access to the provider’s ePHI. A properly written BAA somewhat “protects” the provider if the outside party breaches the ePHI. **Figure 4** [6] shows state BAA presence notated with by the HHS portal with either a “yes” or “no.” The portal reports are not described, so the research below shows the categorical data as posted to the portal.

3. Risk assessment literature and standards

Risk management has been slowly moving into industry. In the United States, HIPAA mandates risk assessment be in place prior to new technology’s being integrated into an organization. Recently, in October 2020, Eddy and Perlrotha [12] reported on a cyber-attack that resulted in a patient death. The attack occurred when “ransomware invaded



30 servers at University Hospital Düsseldorf [...] crashing systems and forcing the hospital to turn away emergency patients.” This is one of the first ransomware-attack-related suspected deaths reported publicly. In such a high-profile and morbid case, we can see the essential importance for having a standardized language for discussing cyber-risks.

3.1 Risk assessment standards

The United States National Institute of Standards and Technologies (NIST) has produced many Special Publications on Risk Assessments [13]. **Figures 5 and 6** [14] show NIST’s generic risk model and risk assessment process respectively. In fact, many organizations around the world are following the NIST Risk Assessment frameworks.

3.2 Automating risk assessments

Risk assessment automation has been proposed in the form of automated penetration testing frameworks [9–11, 13–19]. Testing frameworks and automated tools are extremely useful for detecting known bugs and vulnerabilities. However, in general, these tools do not report on the larger risk-assessment picture. Specifically, they may not accurately report on legal requirements or help an organization prepare for prospective data-breach-associated costs. In addition, there is limited (if any) language standardization on risk findings to enable intra- and inter-organizational risk communication, which is essential for subsequent auditing and legal ramifications.

3.3 Framework libraries for malware and software developments

In addition to developing a standardized framework, NIST and MITRE.org have worked tirelessly to produce a standardized dictionary for attack and malware. For example, they have produced the *Common Attack Pattern Enumeration and Classification (CAPEC)* [20] to classify attacks. NIST maintains the *National Vulnerability Database (NVD)* [21] to identify products with well-known vulnerabilities. In addition to attacks, these organizations are iteratively developing vulnerability dictionaries. For example, MITER sponsors the *Common Weakness Enumeration (CWE)* [22] and NIST sponsors the *Bug Framework (BF)* [23, 24]). These standardized frameworks are purposefully agnostic to vendors, languages, and industry sectors. They have been instrumental and essential for industry, government, and

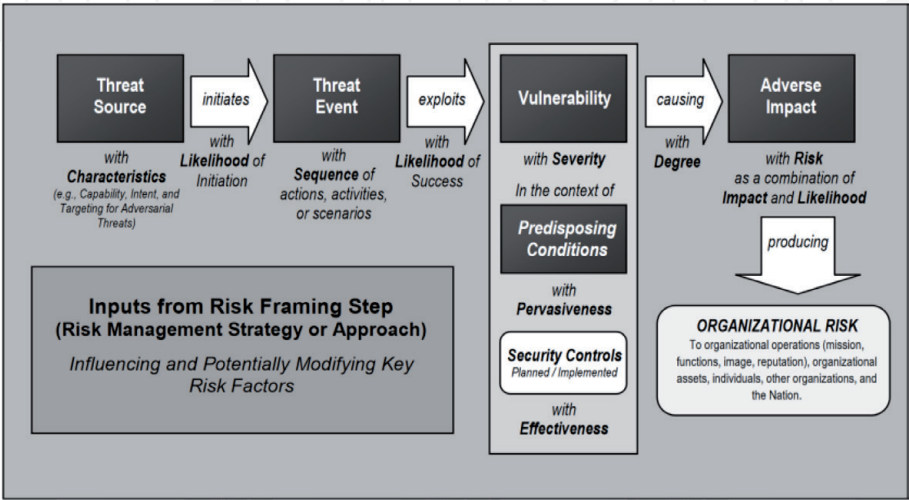
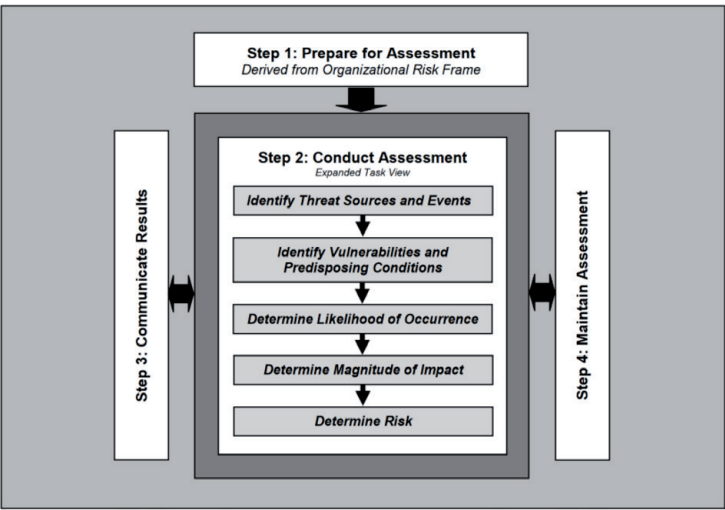


Figure 5.  
NIST’s generic risk model with key risk factors.



**Figure 6.**  
*NIST risk assessment process.*

academia to discuss and communicate software vulnerabilities, assurances, and development techniques. As humans need a standard spoken dictionary to communicate with each other on day-to-day activities, so do they need a similar dictionary to discuss technical activities.

**3.4 Penetration testing reports**

As risk management is still clearly its own type of innovation phase within the technology adoption life-cycle, risk researchers are finding a need to communicate risk through standardized language. For example, let us consider a penetration test report. Historically, there is none of the following: (1) a fixed template, (2) a fixed-strategy, or (3) fixed-finding language. Such non-standardization is subject to extreme bias and misrepresentation. In fact, if every internal or external penetration test is written differently, how can any organization fully understand their own risks? Similarly, if every employee in an organization spoke their own verbal language, how could anything be communicated? Historically, industry has focused on standardizing software vulnerabilities and malicious code patterns. A major gap still exists for risk management components, including budgeting for financial penalties and legal ramifications.

**3.5 Risk assessment education**

Research on risk-assessment education has primarily focused on learning penetration testing techniques [25]. The curriculums discussed in this research neither considers the meta-organizational risk nor risks specifically associated with the medical sector. Schmeelk [26] fills a literature gap by emphasizing that all the risk components should be strategically aligned in terms of standardization.

**4. Risk assessment library considerations**

Managing the risk in a medical setting is unique because of specific regulations that come with significant potential financial fines and corrective actions. For example, outside and inside risk management strategies may not properly align. Also, many organizations, especially in healthcare, are employing a task-based ticketing system to track internal processes. These ticketing systems enable the Information

System silos and other organizational risk components to entirely misalign and improperly manage risk by using neither standardized nor repeatable language.

Schmeelk [26] reports that the following five subsections should be included in identifying organizational components. As a centralized library has yet to be created, a working group should focus on exactly what to include in a standardized public-risk-assessment language dictionary. Important historical components are: legal, training, vendor, and system security requirements, as well as organizational controls. A standardized risk-finding library encourages cross-organizational collaboration, communication, auditing, and legal consistency if a case ever goes to court.

#### **4.1 Regulatory requirements**

Regulatory requirements encompass a wide range of organizational responsibilities, which can be actual governmental laws and/or industry-specific requirements. Let us discuss both.

##### *4.1.1 Industry-specific regulations*

In the United States, medical critical infrastructure entities have both sector-specific regulatory requirements as well as other requirements, such as Payment Card Industry (PCI)-compliance, to consider in risk management [27]. If an organization does not pass PCI (re)compliance auditing, then they are at risk of losing the use of credit cards, among other payment sources under PCI regulations. In the past, organizations would consider themselves a cash-only facility if they lost PCI (re)compliance. Today, with the birth of cryptocurrencies and alternative payment methods not under PCI, losing the use of credit cards might not be as drastic as it has been historically. Other regulations include compliance with those from the International Standards Organization (ISO). Globally, there are many industry-specific regulations that are not necessarily enforceable laws.

##### *4.1.2 Industry-specific Laws*

Medical-covered entities under HIPAA/HITECH are subject to audits by the United States Health and Human Services (HHS) Office of Civil Rights (OCR). The OCR manages many civil rights across the United States in addition to HIPAA. Organizational breaches of patient electronic health information of over 500 individuals must be reported to the OCR as ruled in HITECH. Such breaches are both subject to federal fines and corrective actions. The OCR also can audit covered entities at any point in time. HIPAA is a very well-organized law. It has specific mandates for electronic health data requirements, which should be consistently mapped during a risk assessment to appropriately manage organizational risk. HHS lists many documents for guidance on their website, including mappings between NIST frameworks for cybersecurity and HIPAA requirements. These are extremely useful resources for practitioners.

#### **4.2 Training requirements**

Security education and training awareness (SETA) needs may occur at the vendor level or as federal, state, or city regulations. They are not only legally mandated in many instances for legal responsibilities, but also are ethical mitigations. For example, employing staff who have not been properly trained on data security and then holding them responsible for data security mistakes is unethical. In fact,



in such a case, labor laws may also be violated. Also, in New York State, the loss of employee Social Security Numbers (SSN) through any sort of data breach is a crime subject to legal penalties [28].

#### 4.2.1 Regulation trainings

Different regulations require different levels of SETA. In the credit card industry, organizations using alternatives to cash which are highly-corporately regulated must protect the data by complying with the Payment Card Industry (PCI) regulation. The PCI Data Security Standard (DSS) requires software developers for services using credit cards to be properly trained to code such systems. In addition, federal laws such as HIPAA also have specific training requirements. Lastly, little work on cybersecurity training is being done at state or city levels; however, proper awareness could be suddenly mandated at these local levels. If an organization or their accepted vendors are missing any of these training requirements, the organization may be financially liable.

#### 4.2.2 Best practice trainings

Training based on current best practices is hard to assess because best practices in cybersecurity mean different things to different people and organizations. Training based on best practices is really subjective. Typically in the USA, organizations follow NIST and the Open Web Application Security Project (OWASP) guidance [14, 29]; however, still no industry-wide standards exist for exactly what best practices entail.

### 4.3 Service provider requirements

Service providers and vendors may be subject to different potential cybersecurity risk requirements than the actual provider or covered entity. If a covered entity works with a service provider, it should have proper agreements and risk mitigations in place. Two major sources of such agreements are: business associate agreements (BAAs) and other agreements, such as non-disclosure agreements. Let us examine both in the following subsections.

#### 4.3.1 Business associate agreements (BAAs)

Historically, services providers (or business associates) working with a covered entity's sensitive patient data should have properly formed BAAs in place prior to releasing sensitive data or have a well-formed written legal justification as to why no such BAAs exist. Many HIPAA-covered entities still report breaches where a properly formed BAA was not in place. In such cases, all parties may be considered responsible for the breach by the HHS OCR in the USA.

#### 4.3.2 Non-disclosure agreements and/or other agreements

Business partners may negotiate many different types of agreements and/or partner requirements for their data and products. One popular agreement in healthcare and healthcare research is non-disclosure agreements (NDA). Such agreements require parties not to release information without prior approval. In such a case, malware that makes NDA-protected data public by releasing it on a popular web application du jour, as well as its actual authors, could be faulted to violate the NDA. Cases that fall into this category can have many different negative outcomes, such as legal ramifications, reputational damage, among others.

In addition to NDAs, other Federal or organizational legal regulations may require risk assessments and other services or service-level agreements (SLAs). Similarly, the GDPR requires entities exposed to unauthorized access to notify affected breached individuals within a short timeframe. Violations to such agreements can have extremely negative consequences to the healthcare entities.

#### **4.4 Application and system requirements**

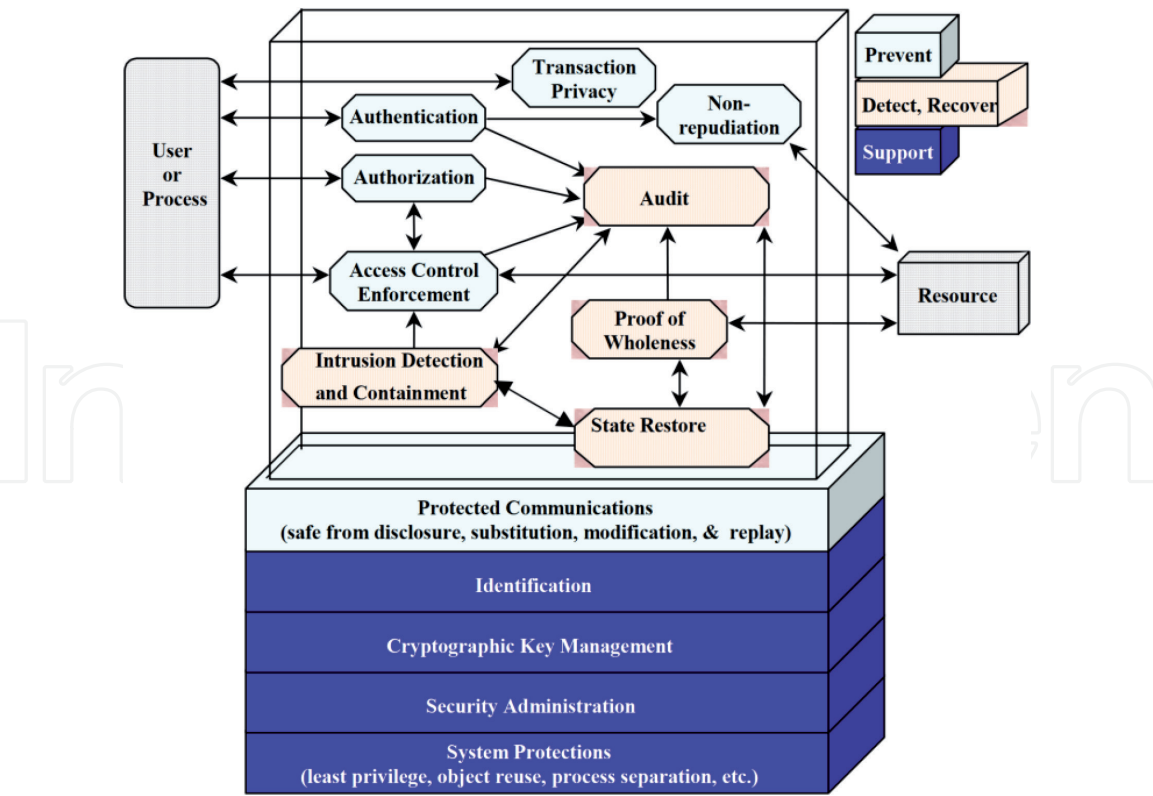
Application and system security are typically measured through certifications (e.g., International Organization for Standardization or other sources) or from internal tests prior to product release. HIPAA requires security assessments for systems and applications managing ePHI. Organizations can either develop their own methodologies to communicate risk that are acceptable by covered entities, or the entities themselves can ask to perform such probability assessments for adverse events. When the covered entity is performing the assessment, they must carefully obtain legal authorization to do so in most cases. In general, Information System silos prevent considering a full-threat landscape for the technical component with the legal, budget, and business use cases. Additionally, digital assessments may be filed for HHS OCR audits into the Integrated Risk Management (IRM) system without updates to the overall business threat mitigations. Periodically, teams must carefully reassess and update the stored organizational predicted levels. In such cases, the assessments are more of a risk “impression” rather than an informed, reproducible, scientific informing on the true likelihood and impact of adverse events. **Figure 7** [30] provides a high-level overview of different technical security controls reported by NIST. The following subsections identify eight subcategories potentially employed during a risk assessment.

##### *4.4.1 Authentication*

According to NIST [30], authentication is the process or action of proving or showing something to be valid. Specifically, “The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid.” The OWASP Application Testing Guide [31] currently gives ten best-practice tests to perform for authentication: “Testing for Credentials Transported over an Encrypted Channel, Testing for Default Credentials, Testing for Weak Lock Out Mechanism, Testing for Bypassing Authentication Schema, Testing for Vulnerable Remember Password, Testing for Browser Cache Weaknesses, Testing for Weak Password Policy, Testing for Weak Security Question Answer, Testing for Weak Password Change or Reset Functionalities, and Testing for Weaker Authentication in Alternative Channel.” It is important to realize that any best-practice guide at-large lists *top* threats and vulnerabilities without perhaps listing *all* threats and vulnerabilities.

##### *4.4.2 Session management*

Session management is the data flow between endpoints—typically following a client and server model. A web session is a series of requests and response transactions created by a client after authentication. In most cases, the endpoints communicate with a special identifier to limit re-authentications. Current best practices in session management include session flags, random token generation, and timeout intervals. The OWASP Application Testing Guide [31] currently lists the following eight session management tests: “Testing for Session Management Schema, Testing for Cookies Attributes, Testing for Session Fixation, Testing



**Figure 7.**  
*Technical security controls.*

for Exposed Session Variables, Testing for Cross Site Request Forgery, Testing for Logout Functionality, Testing Session Timeout, and Testing for Session Puzzling.”

#### 4.4.3 Data-in-transport, data-at-rest, data-in-use

The protection of sensitive information is fundamental to risk management. Data-in-motion is the transfer of material between endpoints. This category changes frequently and includes industry best practices in how to transmit the information, such as confidentiality controls and integrity controls during message transmission. Once information is stored on a system, it is referred to as data-at-rest. Lastly, data-in-use refers to messages in memory. Historically, a concern of data-in-use is that processes and other virtualized components could have improper access to the information.

#### 4.4.4 Authorization and access control

Authorization policies define access capabilities for groups and entities. Access controls, sometimes referred to as permissions or privileges, are mitigating controls to enforce authorization. As such, access controls speak to lowering probabilities against unauthorized access, which could cause loss to data integrity, confidentiality, and availability. The effectiveness and the strength of unauthorized access reduction depend on the correctness of the admittance control decisions and the strength of entry control enforcement. The current OWASP Testing Framework [31] promotes the testing of four key elements in this security area: “Testing Directory Traversal File Include, Testing for Bypassing Authorization Schema, Testing for Privilege Escalation, Testing for Insecure Direct Object References.”

#### *4.4.5 Auditing and monitoring*

Systems and applications should create records for auditing and monitoring. Specifically, archives should be generated before and after critical functions take place. These logs are stored in the system/server backend for regulatory requirements, performance indicators and other analytics. Different components are typically checked during risk management.

#### *4.4.6 Injection and input vulnerabilities*

Injects and input vulnerabilities enable maliciously crafted code to change the underlying intended behavior of a system or application. The OWASP Testing Guide [31] currently lists eighteen common best practice tests, including SQL/NoSQL injection, Cross Site Scripting (XSS), and HTTP injection attacks, among others.

### **4.5 Organizational control requirements**

At the organizational-level, controls such as policies, procedures, physical security and financial budgeting should be considered during an assessment. However, these components of risk management can be managed by entirely different entities.

#### *4.5.1 Policies and procedures*

Organizations should have policies in place [32] at technical, physical, and administrative levels, which are repetitively and consistently followed to avoid different legal ramifications (e.g., from valid discrimination cases to data breaches). Standard operating procedures (SOPs) should also be in place and specifically in writing [32]. Specific procedures, which must be in place at the federal level, include business continuity and disaster recovery plans.

#### *4.5.2 Physical and environmental security*

This component describes the physical and environmental security aspects of the system, if any, which are requirements in the United States Federal HIPAA laws. Physical security encompasses the physical environment to lower the probability of a threat occurring in spaces such as public, private, and shared. It also includes ways to protect organizations from fire and other environmental concerns affecting risk.

#### *4.5.3 Budget for adverse effects*

Risk assessment traditionally includes developing a budget for adverse effects, such as in the Factor Analysis of Information Risk (FAIR) quantitative uncertainty analysis model. Many organizations are not storing-up financial resources in accordance with the uncertain probability being generated to pay for patient identity protections. Digital Guardian [33] has various reports on current costs per record; the costs vary with time. Simply indicating that a system is vulnerable to CSRF may really have no budgetary ramification under certain other conditions. Thus, probability of cost concerns inform on the overall organizational probability of concerns and insurance.

The HHS has historically been responsible for enforcing the Privacy and Security Rules of HIPAA [34]. For most HIPAA covered entities, the HHS OCR



enforcement of the Privacy Rule began April 14, 2003, and the Security Rule began on April 20, 2005. The web portal currently lists government corrective action plans detailing the causes of potential violations of the HIPAA Privacy and Security Rules. Notably, in October 2020, the OCR posted four announcements, most with either sub-cases or multi-breaches, of case settlement with potential corrective action plans for violations to the HIPAA Privacy and Security Rules.

## 5. A risk assessment library

Schmeelk [26] contributed a new open source risk assessment library example to enable researchers, penetration testers, risk assessment managers and institutions to further expand on a consistent risk-assessment findings library with their policies, procedures, organizational controls and legal requirements. As noted in the research bug libraries, dictionaries are being maintained by large organizations but do not include risk-assessment findings, thus complicating risk-management methods. As cited, during experience with internal audits risk assessment, language made analysis next to impossible. For example, modern natural language processing methods would need to take place on penetration tests to evaluate assessment reports among different assessors, each applying different methodologies and terminologies.

### 5.1 Example risk assessment frameworks

Currently, assessment frameworks are entirely intra-organization. In addition, accessing patient databases is impossible—luckily—in the USA due to HIPAA. That said, NIST has guidance on developing an actual risk-assessment process [14]. However, NIST 800–30, as seen in **Figure 5**, does not actually specify threat source, threat event, actual vulnerabilities, or impact. The actual language used to describe these components is entirely left up to each organization to develop. Even worse, each risk assessor on the team may, in fact, describe these components differently (i.e., use entirely different words). In such cases, making any kind of accurate meta-analysis about the organizational risk is entirely impossible. Therefore, we argue that risk assessment frameworks need a standardized library to describe the identified risk.

### 5.2 Example findings library

An open-source library example from Schmeelk [26] is seen in **Figure 8** applying an example-consistent risk language. The library needs to be expanded from industry working groups, similarly to MITER's CWE and NIST's BF.

Some important elements for language specification and risk clarification are seen in **Figure 8** [26]; they are the following: vulnerability short descriptive name, vulnerability expanded description, techniques to remediate or mitigate the vulnerability, estimated likelihood factors, estimated impact factors, related organizational policies/standards, related NIST Controls, related HIPAA regulatory requirements, other related legal requirements such as non-disclosure agreements, and estimated breach cost factors for insurance and related required patient identity-theft protection costs/notifications.

These categories listed in the prototype can arguably be expanded or removed. Historically, vulnerability standardization libraries [20–22] are maintained by major organizations (e.g. MITER) and/or government entities (e.g. NIST). Based on healthcare operation needs, we developed the following descriptions of the prototype categories.



Vulnerability	Description	Remediation	likelihood	Impact	Policy/Standard	NIST Controls	Related HIPAA	Other-Related-Legal	Budget
System does not employ 2-factor authentication	Two-factor authentication is considered industry best practice; something you know, something you are and something you have	Add two-factor authentication	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M - internal only information H - regulated information	NYS-S14-006 - Authentication Tokens	IA-2 : IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	164.312 (c) (2)	Non-Disclosure Agreement (NDA)	L - \$ (\$1K/person) M - \$\$ (\$2K/person) H - \$\$\$ (\$3K/person)
System vulnerable to cross site scripting (XSS)	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.	Output encoding and implement content security policy header.	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or Domain Admins	L - public information M - internal only information H - regulated information	NYS-S13-002 - Secure Coding Standard	SI-10 : INFORMATION INPUT VALIDATION			L - \$ (\$1K/person) M - \$\$ (\$2K/person) H - \$\$\$ (\$3K/person)
System vulnerable to improper password complexity.	A password is a string of characters used to verify the identity of a user during the authentication process.	Enforce more complex passwords on the server-side.	L - < 3 people M - 1-20 patients or < 100 Employees H - 20+ patients, All Employees or	L - public information M - internal only information H - regulated information	NYS-S14-006 - Authentication Tokens	IA-5 : AUTHENTICATOR MANAGEMENT	164.312 (c) (2)	Non-Disclosure Agreement (NDA)	L - \$ (\$1K/person) M - \$\$ (\$2K/person) H - \$\$\$

Figure 8.  
Risk assessment library prototype.

5.2.1 Standardizing the actual risk vulnerability and remediation language

The *vulnerability* column summarizes an identified system, data communication, or application weakness. The *vulnerability description* column gives a community-agreed-on weakness description. The *remediation* column briefly explains known techniques to remediate or mitigate the identified vulnerability.

5.2.2 Standardizing the actual risk likelihood and impact language

The *likelihood* column provides standardized language for estimating the probability of the identified vulnerability exploitation given different threats. Currently every organization makes their own likelihood estimates. Organizations on different “sides of the physical street” with identical systems and surrounding mitigating controls, can label the risk likelihood entirely uniquely. The *impact* category approximates potential resulting consequence levels in the event a vulnerability or finding is realized.

5.2.3 Standardizing the actual risk associated with policies and NIST controls

Historically, organizations should develop policies and standards to help the organization frame their own cybersecurity stance. The NIST Cybersecurity Framework [35] (the NIST CSF Tool is seen in **Figure 9**) is one useful guide for developing an organizational cybersecurity posture and policies/standards.

The category in **Figure 8**, risk assessment library for the NIST controls, is relevant to mapping mitigating controls to well-known NIST vendor agnostic controls. NIST regularly updates the NIST SP 800–30 [14] to account for industry trends.

5.2.4 Standardizing the actual risk to HIPAA requirements

As Security and Privacy Rules of HIPAA are major and enforceable regulatory legislation in the United States, the related column in the library connects the findings to potential HIPAA regulations. This mapping informs the risk-management process when required regulatory elements are entirely missing or are in jeopardy.

5.2.5 Standardizing the actual risk to other industry-specific regulations

Other regulations, such as PCI compliance [27], The Sarbanes-Oxley Act (SOX) of 2002 [36], FTC requirements, service-level agreements (SLAs), state data breach laws [29], and research non-disclosure agreements, can also play their roles in risk

Information Security Risk-Aligned Framework																			
Category	Cybersecurity Framework Control	Priority	Operation Service Group	CIS Top Priority	FDI01.1	FDI01.2	FDI01.3	FDI01.4	FDI01.5	NET Policy	Process Level	Policy Level	Documentation Level	Automation Level	Private Value	Policy Value	Recovery Value	Autonomy Value	Malware Score
Asset Management	Operational Security - Systems	🔴	CMDB Subject: TCM Policy Vulnerability Scanner: CMDB system files (200k)	1, 2	25,000	35,000	10,000	60,000	10,000	DL, DM	Standardized	Informal	Formal	Partial	30%	5%	10%	5%	26.7
	CMDB 1: Physical devices and systems within the organization are inventoried	🔴	CMDB system, Cisco Prime	1							Standardized	Informal	Formal	Partial	30%	5%	10%	5%	100
	CMDB 2: Software definitions and applications within the organization are inventoried	🔴	Vulnerability Scanner, CMDB system	2	10,000	10,000	10,000	10,000	10,000		Standardized	None	Formal	Full	40%	0%	5%	10%	40%
	CMDB 3: Organizational communication and data flows are mapped	🔴	None	1							Standardized	None	Formal	None	10%	0%	10%	0%	100
	CMDB 4: External information systems are catalogued	🔴	CMDB	1	25,000	25,000	0	10,000	0		None	None	None	None	0%	0%	0%	0%	0%
	CMDB 5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	🔴									Standardized	None	Informal	None	10%	0%	5%	0%	100
	CMDB 6: Ownership roles and responsibilities for the entire enterprise and third-party relationships (e.g., suppliers, customers, partners) are established	🔴									Standardized	Informal	None	None	10%	5%	0%	0%	100
Business Environment	Strategic Security - Business Environment	🔴			0	0	0	0	0	AP									36.0
	CBSE 0: The organization's role in the supply chain is identified and communicated	🔴									Standardized	None	None	None	10%	0%	0%	0%	100
	CBSE 2: The organization's place in critical information and its industry sector is identified and communicated	🔴									Standardized	Defined	Formal	Partial	10%	10%	10%	5%	100
	CBSE 3: Priorities for organizational mission, objectives, and activities are established and communicated	🔴									Standardized	None	Development Process	Partial	30%	0%	20%	5%	100
	CBSE 4: Dependencies and critical functions for delivery of critical services are established	🔴									Standardized	Defined	Formal	Partial	10%	10%	10%	5%	40%
	CBSE 5: Business requirements to support delivery of critical services are established for all operating entities (e.g., order fulfillment, during recovery, normal operation)	🔴									Standardized	Defined	Metrics and Reporting	None	10%	10%	10%	0%	40%
Governance	Strategic Security - Governance and Compliance	🔴	Security Policy Security Policy (Standards 002) Security 001		250,000	100,000	100,000	100,000	100,000	All, PL, PM									26.5

**Figure 9.**  
*NIST cybersecurity framework reference tool [35].*

management. For example, SOX “is mandatory. ALL organizations, large and small, MUST comply [36].” Organizations allowing customers to pay with credit cards may directly or indirectly be under PCI compliance. The column *other-related-legal* provides benchmark connections to other generic requirements from these related regulations.

### 5.2.6 Standardizing the actual budget to estimate breach-associated costs

The column on *budget* provides approximate figures for breach and regulation violation ramifications. For example, in 2019, Facebook [37] famously announced a proactive budget appropriation of \$3B with futuristic plans to pay off financial penalties related to regulatory breaches. Surprisingly, in some recent healthcare insurance cases, insurance companies have denied financial payouts for healthcare entity victims for malware-related concerns under “Act of Nature” clauses. Such cases of significant financial losses, where healthcare entities are “on their own” for financially responding to the subsequent effects of the malware or breach, can possibly lead to the healthcare entity’s going out of business.

### 5.3 Performance metrics for an assessment risk framework library

There do exist libraries for software development concerns and known vulnerabilities such as the NIST NVD, NIST Bug Framework, and MITER’s CWE. They assess their performance. MITER provides an analysis of how the library can be used by stakeholders; however, no formal assessment methodologies exist. Assessing a library framework for performance would be like trying to assess the performance of a spoken language. MITER [38] currently lists the following stakeholders of their weakness enumeration (i.e., framework or library): assessment vendors and customers, software developers and, customers, academic researchers, applied vulnerability researchers, refined vulnerability information (RVI) providers, educators, and specialized communities.

According to Schmeelk [26], the library is currently prototyped as a spreadsheet, similarly to the NIST Cybersecurity Framework Reference Tool spreadsheet representation [35]. Currently, each sheet of the spreadsheet refers to specific domains of findings that can be identified during a risk-assessment process. For example, weakness in the physical, technical, or administrative security requirements would each fall on different spreadsheet pages. In addition, each of these three domains can be further broken into subdomains.

## **5.4 Benefits from a standardized risk-assessment framework library**

Currently organizations are developing their own personal language for describing risk. In fact, many risk assessors within the organizations can actually employ their own personal language. When third-party audits and internal audits transpire, there is no way to assess the risk across the risk-assessment reports. For example, one risk-assessor employee could identify a vulnerability as cross-site scripting; whereas, another may document an XSS vulnerability. If the risk has been described differently by all employees, it becomes impossible to identify how many cross-site scripting vulnerabilities really exist within the organization. Hence, the meta-analysis of risk is entirely flawed. As such, it will be improperly conveyed to insurance companies and third-party auditors. Currently, the only way to develop a unified understanding of the risk is to first develop ontologies of potential words used to describe the risk. Then, perhaps aggregate meta-statistics about the organization can be developed by using natural language processing methods on the written reports. For example, modern natural language processing methods would need to take place on penetration tests to evaluate assessment reports among different assessors, each applying different methodologies and terminologies. As such, most insurance companies and third-party auditors are taking large chances on organizations who really do not understand their own cybersecurity concerns.

## **5.5 Improvements made by introducing a standardized risk library**

Currently, there are no other relevant approaches where the risk language is standardized other than the vulnerability language frameworks of MITER and NIST. This lack of standardized risk language remains a major gap in risk analysis. Schmeelk [26] reports on an analysis for the prototype risk library and connects the library to New York State (NYS) Information Technology Security (ITS) Policies [39]. Standardizing the language used during risk assessments is essential for both internal and external factors. First, if a risk-related case ever goes to court, the phrasing of the risk could play a role in the court verdict. For example, if a business chooses to accept a finding where “unauthorized access” was identified during a risk assessment, the organization may be responsible for accepting the risk. Second, when an organization whose assessments have been written using any plethora of words is trying to collect internal metrics, characterizing the current state of cybersecurity within the organization is nearly impossible. This would be a useful application for Natural Language Processing (NLP), trying to characterize quantitatively exact numbers of password violations, XSS, SQL injection, and other findings. Without standardization, knowing at any time an organizational stance on cybersecurity becomes next to impossible. In addition, remediation efforts and risk mitigation efforts are significantly hindered by text-based risk assessments which do not conform to standards. Lastly, if every organization’s employees compose/compile/develop their own libraries, there will be no way to properly coordinate with insurance companies for breach budgeting. Sadly, without any standardization or proper planning, organizations may learn “the hard way” that they are entirely financially responsible for cleaning up a major data breach or ransomware attack.

## **5.6 Industry concerns addressed by a standardized risk library**

The United States and the world are adopting, either explicitly or implicitly, technology-related risk at an unprecedented rate. In addition, regulations are being

adopted across the world at an equally unprecedented rate. In fact, each of the 50 United States and “the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information [29].” Each state law is potentially different from the other state laws, further complicating situations involving out-of-state patients. Most organizations have adopted Integrated Risk Management (IRM) solutions, but many of these solutions require extreme customization from clients. In addition, not everyone in the organization has an overall “view” of the organizational risks. Since Information Systems (IS) trends remain in silos [40], coordinating risk among the different healthcare departments and all the IS sectors is difficult. In addition, entities within an organization that sign off on risk, typically referred to as system owners, may find an imbalance on the risk they must accept on the behalf of the business. Then, as system owners leave or retire from an organization, subsequent new hires may not fully understand the risks inherited with their positions. In fact, new hires in security high-level positions often ask the organization for audits prior to taking, or during the first year of, a new job. That way they can benchmark the inherited risks.

## 6. Conclusions


As risk management evolves, so do the needs for risk communication and risk articulation. Healthcare entities need to know, in advance, exactly what their insurance covers involving privacy and security risks. Patients need to be aware of identity theft concerns if their personal identifying information (PII) is breached and sold in alternative marketplaces. Technology in the healthcare-related infrastructure is here to stay; ultimately, society will need to standardize how they deal with and respond to privacy and cybersecurity risks. The sooner we adopt a framework of actual privacy and security violations and corrections, the better industry will be able to communicate and mitigate risks—especially in healthcare where human life is at ultimately at risk.

### Author details

Suzanna Schmeelk  
St. John's University, New York, USA

\*Address all correspondence to: [schmeels@stjohns.edu](mailto:schmeels@stjohns.edu)

### IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 



## References

- [1] Europe Union (2020) The EU General Data Protection Regulation (GDPR). Retrieved from: <https://eugdpr.org>
- [2] Maranto, Lauren (2020) Who Benefits from China's Cybersecurity Laws? Retrieved from: <https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws>
- [3] U.S. Department of Health and Human Services (HHS). (2020). Health Information Privacy, from <https://www.hhs.gov/hipaa/index.html>
- [4] U.S. Department of Health and Human Services (HHS). (2013, July 26). HITECH Act Breach Notification Guidance and Request for Public Comment. Retrieved July 11, 2020, from <https://www.hhs.gov/hipaa/for-professionals/security/guidance/hitech-act-breach-notification-guidance/index.html>
- [5] Federal Trade Commission (2020) Health Breach Notification Rule. Retrieved from: <https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule>
- [6] Schmeelk, S. (2019). Where is the Risk? Analysis of Government Reported Patient Medical Data Breaches. In IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume (WI '19 Companion). Association for Computing Machinery. New York, NY. doi:<https://dl.acm.org/doi/10.1145/3358695.3361754>
- [7] Schmeelk, S. (2019). Identity Theft: Anatomy of a Data Breach. New York, New York: Parsons - The New School for Design. URL <https://parsons.nyc/thesis-2019>
- [8] M. Catelani, L. Ciani and C. Risaliti, "Risk assessment in the use of medical devices: A proposal to evaluate the impact of the human factor," 2014 IEEE International Symposium on Medical Measurements and Applications (MeMeA), Lisboa, 2014, pp. 1-6.
- [9] F. Kammüller, "Combining Secure System Design with Risk Assessment for IoT Healthcare Systems," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 2019, pp. 961-966.
- [10] Sonia H. Stephens. 2015. Interactive data visualization for risk assessment: can there be too much user agency?. In Proceedings of the 33rd Annual International Conference on the Design of Communication (SIGDOC '15). ACM, New York, NY, USA, Article 9 , 2 pages. DOI: <http://dx.doi.org/10.1145/2775441.2775446>
- [11] Schmeelk, S., Dragos, D., & DeBello, J. (2021). What Can We Learn about Healthcare IT Risk from HITECH? Risk Lessons Learned from the US HHS OCR Breach Portal. Hawaii International Conference on System Sciences-54 (Under review) (p. 10). Kuai, HI, USA: University of Hawaii at Manoa.
- [12] Eddy, M. and Perlroth, N. (2020) Cyber Attack Suspected in German Woman's Death Retrieved from: <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomware-death.html>
- [13] U.S. NIST (2020) Cybersecurity Resource Center. Retrieved from: <https://csrc.nist.gov/Topics/Security-and-Privacy/risk-management/risk-assessment>
- [14] U.S. NIST (2012) NIST Special Publication 800-30. Guide for Conducting Risk Assessments. Retrieved from: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>



- [15] B. Xing, L. Gao, J. Zhang and D. Sun, "Design and Implementation of an XML-Based Penetration Testing System," 2010 International Symposium on Intelligence Information Processing and Trusted Computing, Huanggang, 2010, pp. 224-229.
- [16] K. P. Haubris and J. J. Pauli, "Improving the Efficiency and Effectiveness of Penetration Test Automation," 2013 10th International Conference on Information Technology: New Generations, Las Vegas, NV, 2013, pp. 387-391.
- [17] H. Radwan and K. Prole, "Code Pulse: Real-time code coverage for penetration testing activities," 2015 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2015, pp. 1-6.
- [18] Lei Liu, Jing Xu, Chenkai Guo, Jiehui Kang, Sihan Xu and Biao Zhang, "Exposing SQL Injection Vulnerability through Penetration Test based on Finite State Machine," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 1171-1175. doi: 10.1109/CompComm.2016.7924889
- [19] A. Blome, M. Ochoa, K. Li, M. Peroli and M. T. Dashti, "VERA: A Flexible Model-Based Vulnerability Testing Tool," 2013 IEEE Sixth International Conference on Software Testing, Verification and Validation, Luxembourg, 2013, pp. 471-478.
- [20] MITRE (2020) Common Attack Pattern Enumeration and Classification. Retrieved from <https://capec.mitre.org>
- [21] NIST (2020) National Vulnerability Database. Retrieved from: <https://nvd.nist.gov>
- [22] MITRE (2020) Common Weakness Enumeration. Retrieved from: <https://cwe.mitre.org>
- [23] I. Bojanova, P. E. Black, Y. Yesha and Y. Wu, "The Bugs Framework (BF): A Structured Approach to Express Bugs," 2016 IEEE International Conference on Software Quality, Reliability and Security (QRS), Vienna, 2016, pp. 175-182. doi: 10.1109/QRS.2016.29
- [24] NIST (2020) Bug Framework. Retrieved from: <https://samate.nist.gov/BF>
- [25] Lee Epling, Brandon Hinkel and Yi Hu. 2015. Penetration testing in a box. In Proceedings of the 2015 Information Security Curriculum Development Conference (InfoSec '15). ACM, New York, NY, USA, Article 6, 4 pages. DOI: <https://doi.org/10.1145/2885990.2885996>
- [26] Schmeelk, S. (2020) Creating a Standardized Risk Assessment Framework Library for Healthcare Information Technology, HICSS-53: Hawaii International Conference on System Sciences, DOI: 10.24251/HICSS.2020.474
- [27] PCI Security Standards Council (2020). Securing the Future of Payments Together. Retrieved from: <https://www.pcisecuritystandards.org>
- [28] New York State (2020) New York State Social Security Number Protection Law. Retrieved from: [https://www.albany.edu/ampra/assets/New\\_York\\_Social\\_Security\\_Number\\_Protection\\_Law.pdf](https://www.albany.edu/ampra/assets/New_York_Social_Security_Number_Protection_Law.pdf)
- [29] NCSL (2020) Security Breach Notification Laws. Retrieved from: <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>
- [30] U.S. NIST (2002). Risk Management Guide for Information Technology Systems. Retrieved from: <https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01>

[31] OWASP (2020) OWASP Testing Guide. Retrieved from: <https://owasp.org/www-project-web-security-testing-guide>

[32] Santos, O. (2019). Developing cybersecurity programs and policies.

[33] Digital Guardian (2019) What's the Cost of a Data Breach in 2019? Retrieved from: <https://digitalguardian.com/blog/whats-cost-data-breach-2019>

[34] HHS (2020) HIPAA Enforcement. Retrieved from: <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html>

[35] NIST (2020) NIST Cybersecurity Framework. Retrieved from: <https://www.nist.gov/cyberframework>

[36] SOX Law (2020) Sarbanes-Oxley Act of 2002 Retrieved from: <https://www.soxlaw.com>

[37] Jeff Horwitz (2019) Facebook Sets Aside \$3 Billion to Cover Expected FTC Fine. Retrieved from: <https://www.wsj.com/articles/facebook-sets-aside-3-billion-to-cover-expected-ftc-fine-11556137113>

[38] MITRE (2020) CWE Stakeholder Analysis. Retrieved from: <https://cwe.mitre.org/community/research/stakeholders.html>

[39] New York State (2020) ITS Security Policies. Retrieved from: <https://its.ny.gov/eiso/policies/security>

[40] Benson, R.J., Ribbers, P.M., and Blitstein, R.B. (2014) Preface and Chapter 1. Trust and Partnership: Strategic IT: Management for Turbulent Times. Wiley. 1118443934