CSEC630 Med-A Clinic Risk Assessment

(Med-A Clinic is a fictitious clinic)

Megan Bell

University of Maryland University College

October 30, 2016

Author's Note

This paper was prepared for CSEC 630 Prevention and Protection Strategies in Cybersecurity, taught by Professor Ye Tung.

This evaluation is based on a fictitious medical clinic named Med-A clinic. I developed this case study based on years of working with numerous healthcare organizations and across a diversity of healthcare and medical/ clinical research data projects. Data and findings for the fictitious clinic were derived and not based on actual data. I chose UCSF because of their exceptional commitment to information security and privacy. The information presented for UCSF was drawn from public information sources.

Abstract

Med-A clinic is a medical practice that specializes in geriatric medical care, research, and treatment innovation. Med-A is recognized for their innovations and is interested in partnering with the University of California – San Francisco (UCSF) for geriatric research and groundbreaking treatment. Med-A was required to conduct a security risk assessment as part of the due diligence process for UCSF. Med-A has an information security program that is maintained by an outsourced IT firm. The outsourced IT firm has implemented a network security perimeter, encryption, and local computer security protections. With a lack of experience in data breach events and weak incident response planning, Med-A's risk assessment focused on a broad range of vulnerabilities and potential threats that could result in compromise. The NIST risk assessment approach identified in NIST publication 800-30 was used to conduct a risk assessment. Gaps in Med-A's information security program and data breach handling experience were supplemented through industry research and issue analysis relative to UCSF data breach incidents. Recommendations for Med-A focus on maturing an existing information security program where employees are the vulnerability.

Table of Contents

CSEC630 IA1: Med-A Clinic Risk Assessment

Introduction

A medical healthcare clinic referred to as Med-A is a San Francisco medical practice that specializes in geriatric care. The name of the firm has been altered to protect privacy of organization. Med-A has a reputation for conducting geriatric research and is applying for a long-term contract with the University of California – San Francisco (UCSF) for geriatric treatment. The contract could have significant business opportunity for Med-A and its future growth.

UCSF requires its partners to complete sustentative legal, business and technical documentation as part of the due diligence process for business partners. One of the requirements is a security risk assessment. Med-A must also have a cyber-insurance policy and must provide proof of cyber-insurance as part of an application process (Valacich & Schneider, 2016). UCSF's requirements stem from legal oversight under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) (Regan, 2009). Med-A also is regulated by HIPAA and HITRUST.

The security risk assessment results presented in this paper detail the process of evaluating Med-A information security program and the benefits that risk assessments provide in ensuring the confidentiality, integrity, and availability of Personally Identifiable Information (PII) and Protected Health Information (PHI). The risk assessment includes a discussion of risk framework selection and review of trends in information security risk. Threat and vulnerability analysis results are discussed followed by the resulted of risk determination. Finally, recommendations and countermeasures are provided to strengthen the existing information security program.

Med-A Physical Security and Information Systems

Med-A clinic occupies an upper-level location in a medical offices building that has no building-level security to control public access. The building has been earthquake retrofitted and has mandatory fire-protections. Nightly cleaning staff is outsourced. The office layout has an office lobby with a door that limits access to back office medical facilities. Offices where patient data and accounting records are likely to be used are restricted to rooms with keyed locks; doors are open during business hours.

Med-A clinic employs outsourced IT staff to manage their information systems. Office computers have Microsoft Windows Operating Systems (OS), and centralized servers for file storage, databases, and electronic health records (EHR) have use Windows OS with encryption. Each computer has Symantec endpoint protection, which includes encryption, anti-virus and firewall protections. Email is outsourced. The firewall is part of a Barracuda security appliance that also provides virtual private network (VPN), intrusion detection, and intrusion protection capabilities. The outsourced IT group has remote access capability to VPN into Med-A clinic. There is one employee who oversees the EHR system and patient management software. An accountant has additional software for managing book keeping.

Risk Assessment Methodology

Risk assessment involves risk identification, analysis, and evaluation (Vacca, 2013). The risk assessment process begins with an understanding of the organization's assets and their value to the organization. Assets may be physical items such as computers or intangible assets such as the potential value of a patent. After asset enumeration, risk identification takes place through the

threat modeling process. The threat modeling process permits an organization to identify and review a range of potential threats types, which are outlined in Appendix A. Threats are analyzed in context of vulnerabilities, and identified risks are evaluated for risk reduction (Valacich & Schneider, 2016).

Med-A requested stressed the importance of addressing the importance of protecting the confidentiality of patient data. Confidentiality was critical to Med-A business and reputation. The information systems that host and process patient data are collectively significant assets. All computers are important since all computers touch, handle or store patient data. A compromise of one computer could result in the loss of confidentiality in patient data.

Risk Framework Selection

Risk frameworks exist to provide structure for risk assessment and management (Freund & Jones, 2015). In healthcare, a risk framework must address a myriad of federal, state, and regulatory requirements by providing structure that facilitates use of "reasonable and appropriate" safeguards in the protection of patients and their data (HITRUST, 2003). For the Med-A clinic risk assessment, the NIST Risk Management Framework (RMF) methodology was selected for its comprehensiveness and availability of templates and examples to facilitate the risk assessment process. It was important to select an industry-accepted framework that addressed healthcare industry requirements and met the high standards associated with UCSF's data security.

Existing Information Security Program Review

Prior Risk Assessments

Med-A clinic conducted its prior security risk assessments using a tool known as Security Assessment (SRA) tool (Office of the National Coordinator for Health Information Technology [ONC], n.d.). Risk assessments were required for compliance with a federal government program known as Meaningful Use which was a government program that financially subsidized upgrading electronic health record technology (Centers for Medicare & Medicaid Services [CMS], n.d.). SRA enabled the creation of security program documentation, but Med-A lacked a formal risk program and framework for managing information security risk. There were gaps in physical security and lack of focus on factors such as fraud.

Documentation Review

Information security documentation developed in conjunction with Med-A's Meaningful Use program was reviewed. The SRA tool enabled Med-A clinic to conduct systems characterization and complete high level threat and vulnerability analysis. Documentation centered on the EHR software and its use rather than all information systems. Incident response, business continuity, and disaster recovery plans were considered nascent in that documentation was likely to contain template language rather than language that was crafted for Med-A clinic. Med-A clinic had never tested their documentation for a possible security incident.

Threat Analysis

Med-A began its threat analysis with prior risk assessments evaluation, security

documentation review, and its industry-focused review on healthcare information security risks and UCSF-historic security incidents that were publically reported. Following detailed analysis, Med-A clinic was able to conduct threat analysis as outlined in the NIST RMF.

Healthcare Industry Risk Profile

Med-A clinic did not have a history of security incidents. In planning the risk assessment, a decision was made to evaluate broader trends in information security incidents associated with data breaches and also to review UCSF's public profile of security incidents. The evaluation of known UCSF security incidents was considered important to addressing particular concerns that UCSF would have in its review of Med-A clinic's security posture. Prior industry analysis was initiated with review of breach notifications where healthcare organizations subjected to HIPAA regulation are required to publically report breaches with greater than 500 individuals (Regan, 2009).

Publically available data from the U.S. Department of Health and Human Services Office for Civil Rights [OCR] was downloaded and analyzed to obtain an overview of causes of data breach events and sources of lost or compromised data (OCR, n.d.). In Appendix D, theft and unauthorized disclosure were the largest singular sources of data breach events. As displayed in Appendix E, paper/film and laptop devices were the primary sources of compromised data. Examples of data breach events involving paper/film include patient records thrown in the trash without shredding or printing insurance PHI on the outside of envelopes. Device theft and unauthorized access were further analyzed with respect to UCSF to further identify potential threats and vulnerabilities.

Device theft.

According to OCR data, theft of laptops and other devices is a primary source of risk for healthcare data breaches, and UCSF has suffered a small number of these breaches. Between 2009 and 2014, UCSF experienced five data breach events that involved notification to OCR for records containing regulated PHI for more than 500 individuals. As observed in Table 1, four of the five events involved theft of laptops or desktops. Review of the specific events indicated that at least two of these incidents involved patient data that was stored without encryption protection (Goldman, 2014).

Table 1

OCR Notifications of UCF Data Breaches with Greater then 500 Individuals

Breach Submission Date	Type of Breach	Location of Breached Information	Individuals Affected
12/15/2009	Other	Email	610
01/27/2010	Theft	Laptop	7,300
10/03/2013	Theft	Laptop, Paper/Films	3,553
11/22/2013	Theft	Laptop, Paper/Films	8,294
03/12/2014	Theft	Desktop Computer	9,861

Unauthorized exposure or misappropriation of data.

According to OCR (n.d.), OCR-tracked data breach notifications document unauthorized access to patient data as the second main source of data breach events. One Table 1 item is a December 15, 2009 data breach event involving email. Kaarlela (2009) reported that was a doctor's email was compromised in spear phishing scam where an email was crafted as coming from UCSF's information security group that requested the doctor's UCSF login credentials.

External threat actor concerns.

While UCSF suffered a spear-phishing attack as described above, there are no recent

publically reported instances of data breach events involving threat actors such as hackers and the implications of malware. According to Symantec (2016), millions of new malware were detected in 2015. Of particular interest to Med-A is ransomware, which increased 35 in 2015. External attackers may include organized crime or nation-states. Symantec's findings are consistent in healthcare where cyberattacks such as Anthem and Premera BlueCross (HIPAA Journal, 2016).

Threat Source and Event Analysis.

Threat source review.

A listing of approximately 120 threat sources was compiled. Threat sources were derived from multiple sources such as NIST RMF documentation and OCR-documented data breach events (NIST, 2012; U.S. Department of Health and Human Services Office for Civil Rights [OCR], n.d.). As discussed in Appendix A risk methodology and in Appendix B, threat sources were characterized as being in-scope of assessment. About 55 threat sources were considered for further analysis. Next, threat associated with individuals or other entities were evaluated.

Results from threat source analysis indicated there were few high likelihood sources that could have the sophistication and knowledge to execute a highly successful threat event. Privileged insiders with extensive knowledge of Med-A's business and security practices and hackers with advanced capabilities for authentication bypass or the ability to deploy malware were considered highest risk threat sources. Hackers associated with organized crime were considered the most plausible threat sources. Malware was a considered a critical threat source as a tool associated with potential compromise.

Threat event analysis.

Determination of threat events for analysis required more than three iterations to develop experience with threat event analysis. More than 75 threat events were included in the final threat event analysis. As check against consistency of results, about three duplicate events were included. As discussed in Appendix A, threat events were assessed for relevance.

Med-A clinic had six prior identified risk incidents that were rated as confirmed for relevance in the risk assessment. These incidents included writing down passwords and patient PHI on paper in unsecured areas, clicking on links in spam emails, one recalled incident of potential browser hijacking by adware, and hard disk failure in a desktop computer.

During secondary analysis of threat events associated with higher ratings for capability, intent, and targeting, it was observed that many potentially serious threats would likely have low probabilities of occurrence. However, the higher ratings resulted in discussions of believability in risk assessment results. In moving to further likelihood and level of impact determinations, example scenarios continued to provide a valuable baseline for resulting metrics.

Vulnerability Assessment

Vulnerability assessment was performed in accordance with the NIST RMF as summarized in Appendix A. Prior security documentation and risk assessment results were used. The threat-centric focus of the NIST RMF limited direct vulnerability analysis to severity ratings. About 75 vulnerabilities were rated on a scale with qualitative ratings of Very Low, Low, Moderate, High, and Very High. The highest severity vulnerability rating was High, and

nine vulnerabilities were identified with a rating of High. The nine vulnerabilities are listed in Appendix E. External device use for storing and transporting electronic data was observed as the most significant vulnerability. Unsecured paper records were identified as vulnerability, but they were not considered to have the same level of risk as electronic records. Internet use and the ability to connect personal devices such as an iPhone were also identified. From a vulnerability perspective, specific file servers and network connections were not perceived to be vulnerable. Results of vulnerability analysis also reflected reliance on outsourced IT services and the determination of hardware and software vulnerabilities.

Risk Determination

Risk determination analysis incorporates the final analysis of likelihood establishment for event initiation, adverse events, and level of impact. Med-A's existing information security program has a foundation of protection that includes encryption to protect PII and PHI and utilizes layered security such as a network defense perimeter. Med-A's challenge is to reduce people-related risks and further strengthen information systems through upgrading and better policy and patching automated practices.

Likelihood of initiation / adverse events.

Appendix F presents results for the top twenty threat events identified as having the greatest possible consequences for Med-A clinic. Top threat events included natural disasters, device loss of unencrypted devices containing PHI, unauthorized access to patient records such as improper viewing of records, and successful exploitations by external actors such as hackers. Targeted attacks by hackers were identified as having the greatest possible negative impact for Med-A.

While Med-A has not been previously compromised, this risk is consistent with the broader healthcare industry risk profile established earlier in this assessment.

Level of Impact

Fourteen out of the top twenty threat events analyzed had moderate impact ratings. The high number of moderate ratings existed due to threat events being likely to have a possible range of impacts based on risk-scenario factors. Med-A clinic believed that use of a moderate rating provided for a consistent midpoint ranking enabled better discussions to address unknown risks.

Med-A clinic employed the results from its investigation of UCSF public security incidents to assess level of impact for lost devices that hosted unencrypted patient data. Since these events were publically reported, it was assumed that incident response procedures were followed in post-incident analysis and determination of the number of affected individuals. For example, UCSF has a comprehensive incident response plan and several publically available procedures such as incident investigation (UCSF, 2012).

Final Likelihood Determination and Ranking

Risk determination and ranking of risks were the final phase of risk assessment analysis. Risk determination was completed following NIST RMF procedures that are summarized in Appendix A. The NIST ratings table used to transform threat likelihood and level of impact to a risk determination is presented in Appendix I.

The ten risks with the highest risk determinations and ranking are displayed in the second table of Appendix H. Top risks demonstrate two consistent themes of patient data compromise and

adverse impacts to Med-A's clinical and information systems. While hackers have not previously compromised Med-A's information systems, data breaches involving hackers were considered a threat requiring attention due to increased cyberattacks in all industries including the healthcare industry (Symantec, 2016).

Recommendations and Countermeasures

This section addresses recommendations and countermeasures associated with the information security risk assessment (Bayne, 2002; Norman, 2009).

Incident Response Plan

Med-A was identified as having limited incident response plan documentation and had never experienced a significant data breach event. It is recommended that Med-A work with an information security expert to evaluate and update its information security response plan as well as related disaster recovery and business continuity plans (Vacca, 2013). An incident response addresses the legal requirements of HIPAA and HITRUST and facilitates compliance with state-level laws for the protection of regulated data (Swire & Ahmad, 2011).

Restriction of Personal Device Use

It was observed that personal devices were a risk to the confidentiality of patient data and Med-A clinical research. To remediate this vulnerability, it is recommended that specific security policies such as bring your own device (BYOD) policies be created (Vacca, 2013). The BYOD policy should state that personal external devices cannot be connected to Med-A computers.

Encryption

In addition to BYOD, an encryption policy should exist for all devices to protect the confidentiality and integrity of all data while at rest, in transit or in use (Vacca, 2013; Swire & Ahmad, 2011).

Hackers and Malware Concerns and Benefits of Layered Security

Med-A's IT firm maintains IT infrastructure and practices layered security. Med-A's has a developed network perimeter defense such as firewall with intrusion prevention technology (UMUC, n.d.). Local computers employ Symantec endpoint security protection. Med-A's overall security has a reduce likelihood of malware infection and network intrusion through hacking due to these defensive measures.

Med-A's layered security approach could be strengthened with better IT controls and information security policies that could be enforced through centralized access controls (Goodrich & Tamassia, 2011).

Centralized Access Controls

Outsourced IT has recommended Microsoft Active Directory implementation for role-based access controls (Antur, Sawhney, Puri, & Bisht, 2001). Role-based access controls would allow the deployment of group role-based access controls (RBAC) and security policies (Goodrish & Tamassia, 2011). RBAC can implement controls such limited file and folder access.

Employee Training

Employee training reinforces information security policies and in some cases is required as part of an information security program. UCSF requires mandatory training and hosts special events such as compliance week to further develop awareness security (UCSF News Service, 2016). A formal training program would demonstrate alliance with UCSF practices.

Social engineering is a primary source of compromise for malware and network intrusions (Symantec, 2016). Training employees on how to review email for signs of phishing and intentional targeting is important to reducing social engineering attacks.

Password Management

The IT outsourcing firm and Med-A indicated that employees controlled their passwords. Med-A should develop a password management program that removes the control of passwords from employees. This reduces the risk of poor password hygiene to the confidentiality, integrity, and availability of patient data (Goodrich & Tamassia, 2012; Vacca, 2013).

Patching

The IT outsourcing firm and Med-A indicated that patching was regularly performed on all systems. Patching is the process of updating computer systems firmware and software (Vacca, 2013). Patching appeared to be a manual process, which can lead to cumbersome efforts to maintain current patching. The outsourced IT firms may consider the use of automated patching for streamlining the frequency of updates.

Penetration Testing

Penetration testing is recommended as to locate further possible vulnerabilities that culd lead to stronger network and application risk reduction (Vacca, 2013).

References

Antur, A. K., Sawhney, S., Puri, H., & Bisht, N. S. (2001). U.S. Patent No. 6,212,558. Washington, DC: U.S. Patent and Trademark Office.

Babcock, C. (2014, March 3). 9 Worst Cloud Security Threats - InformationWeek. Retrieved from http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085?page_number=2

Bayne, J. (2002). An overview of threat and risk assessment. Bethesda, MD: SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

Centers for Medicare & Medicaid Services (CMS). (n.d.). EHR incentives & certification: How to attain Meaningful Use. HealthIT.gov. Retrieved from https://www.healthit.gov/providers-professionals/how-attain-meaningful-use

Freund, J., & Jones, J. (2013). Measuring and managing information risk: a FAIR approach. Butterworth-Heinemann.

Goodrich, M. T., & Tamassia, R. (2011). Introduction to computer security. Boston: Pearson.

Goldman, J. (2014, March 13). UCSF Medical Center admits third data breach in four months. *eSecurity Planet*. Retrieved from http://www.esecurityplanet.com/network-security/ucsf-medical-center-admits-third-data-breach-in-four-months.html

HIPAA Journal. (2016, July 10). Major 2016 healthcare data breaches: Mid year summary. Retrieved from http://www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/

HITRUST Alliance. (2013). Risk management frameworks. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/HITRUST-RMF-Whitepaper-2015.pdf

Kaarlela, C. (2009, December 15). UCSF notifies patients and other individuals of possible unauthorized access to personal information. Retrieved from https://www.ucsf.edu/news/2009/12/4338/ucsf-notifies-patients-and-other-individuals-possible-unauthorized-acces

Landoll, D. J., & Landoll, D. (2005). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC Press.

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector.

National Institute of Science and Technology. (2012). Common vulnerability scoring system version 2 calculator - CVE-2008-4250. Retrieved from https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-

4250&vector=%28AV%3AN%2FAC%3AL%2FAu%3AN%2FC%3AC%2FI%3AC%2FA%3AC%29

National Institute of Science and Technology. (2012). Special publication 800-30 revision 1. Guide for conducing risk assessments. Washington, DC: U.S. Department of Commerce. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Norman, T. L. (2009). Countermeasure Goals and Strategies. *Risk Analysis and Security Countermeasure Selection,* 247-264. doi:]

Regan, P. M. (2009). Federal Security Breach Notifications: Politics and Approaches. *Berkeley Technology Law Journal*, *24*(3), 1103-1132.

Swire, P. P., & Ahmad, K. (2011). U.S. private-sector privacy: Law and practice for information privacy professionals. NH: International Association of Privacy Professionals.

Symantec Corporation. (2016, April). 2016 Symantec Internet security threat report (Volume *21)*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/.../istr-21-2016-en.pdf

The Open Web Application Security Project (OWASP). (2010). The ten most critical web application security risks. Retrieved from https://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

Thibodeau, P. (2016, September 07). University of California hires India-based IT outsourcer, lays off tech workers. Retrieved from http://www.computerworld.com/article/3117602/it-outsourcing/university-of-california-to-send-some-it-jobs-to-india.html

UcedaVelez, T., & Morana, M. M. (2015). Risk centric threat modeling: Process for attack simulation and threat analysis. John Wiley & Sons.

UCSF News Service. (2016, September 20). UCSF plans events for National Cyber Security Awareness month. Retrieved from https://www.ucsf.edu/news/2016/09/404266/ucsf-plans-events-national-cyber-security-awareness-month

UCSF. (2012, August). UCSF incident investigation procedures. Retrieved from https://it.ucsf.edu/policies/ucsf-incident-investigation-procedures

UCSF (n.d.). Certificates of insurance (online manual). Retrieved from http://rmis.ucsf.edu/certificates-insurance

UMUC. (n.d.). Enterprise network intrusion prevention systems: Prevention and protection strategies in cybersecurity [Interactive module]. MD, USA: UMUC.U.S. Department of Health and Human Services Office for Civil Rights. (n.d.). Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Office of the National Coordinator for Health Information Technology (ONC). (n.d.). Security Risk Assessment tool (Version 1) [Computer software]. Retrieved from https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Vacca, J. R. (2013). Computer and information security handbook (Second ed.). Amsterdam: Elsevier.

Valacich, J. S., Schneider, C., & Jessup, L. M. (2016). Information systems today: Managing in the digital world. Prentice Hall.

Vellani, K. H. (2005). Strategic security management: risk assessments in the environment of care. *Journal of healthcare protection management: publication of the International Association for Hospital Security*, *22*(2), 70-78.

Appendix A

Risk Assessment Methodology

Risk Assessment and Metrics

A comprehensive risk program should consider a broad risk assessment process as presented in Figure 2 ((Vellani, 2005). Risk assessments should also encompass the existing security measures. Risk assessments should include the security function as well as legal, operational, insurance, health, and safety staff. In addition, traditional risk assessment methodology should account for mature organizations with developed information security programs.

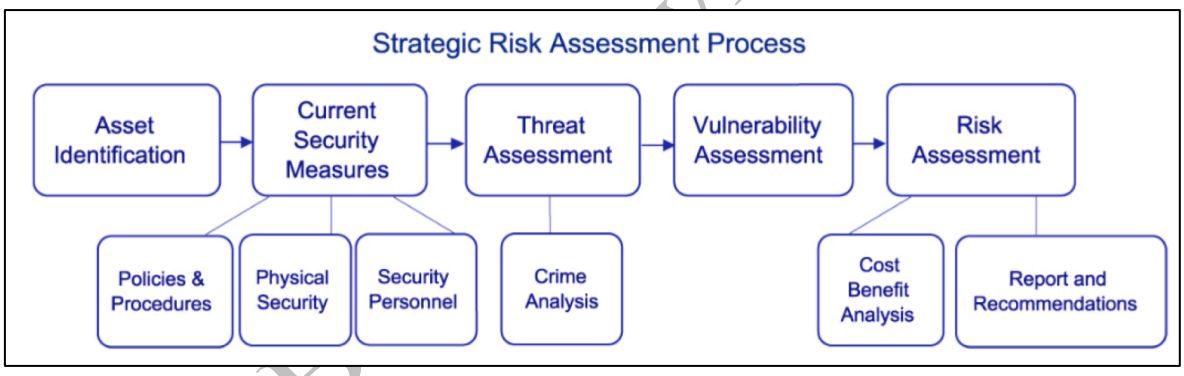


Figure 2. Strategic risk assessment process from The Threat Analysis Group, LLC. Reprinted from *Journal of healthcare protection management* (p. 70-78), by International Association for Hospital Security, 2005.

Risk assessment involves risk identification, analysis, and evaluation (Vacca, 2013). The risk assessment process begins with an understanding of the organization's assets and their value to the organization. Assets may be physical items such as computers or intangible assets such as the potential value of a patent. After asset enumeration, risk identification takes place through the

threat modeling process. The threat modeling process permits an organization to identify and review a range of potential threats types, which are outlined in Appendix B. Threats are analyzed in context of vulnerabilities, and identified risks are evaluated for risk reduction (Valacich & Schneider, 2016).

Consistent risk assessment involves the use of a structured approach and application of quantitative or qualitative ratings (NIST, 2012). Quantitative and qualitative rating scales involve inherent flaws in use which include mis-interpretation of meaning. For example, the selection of Likely versus Highly Likely ratings on a qualitative scale depends on the clarity of rating definitions and experience with applying ratings (Freund & Jones, 2013). Ideally, a quantitative approach is used that accounts for factors such as number of times an event occurs or number of outages resulting from power loss. Organizations should assess the types of metrics and rating scales that are appropriate for a specific risk assessment (NIST, 2012).

The NIST Risk Management Framework (RMF) was employed for risk assessment. NIST (2012) provided for qualitative assessments where the qualitative scales were correlated to numeric values. This assessment utilized a qualitative ratings approach and considered potential issues in ratings through mapped quantitative metrics as needed. As observed in Figure 1, NIST's model for risk assessment incorporates threat modeling, vulnerability analysis, and risk likelihood determination based on the potential impact from an incident (NIST, 2012).

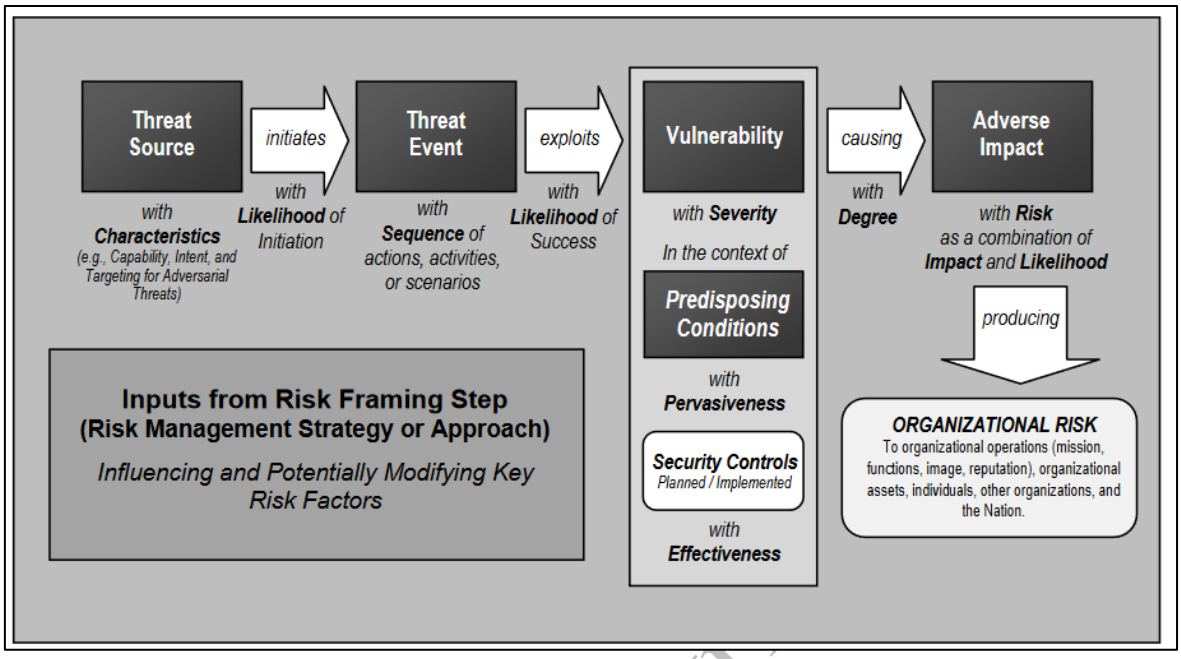


Figure 1. Security risk model from NIST 800-30. Reprinted from *Guide to Conducting Risk Assessments* (p. 7), by NIST, 2013, Department of Commerce. Reprinted with permission.

Threat Source Analysis

Threat modeling is a multi-step process that involves threat source identification and classification, specific threat event enumeration, and relevance to an organization (NIST, 2012). NIST recommends that threat assessment take place in context of the potential harm to an organization.

Threat source assessment.

Threat modeling begins with identification of threat sources that are in scope for an organization. NIST (2012) provides a listing of threat sources and also recommend an organization review its business and technical environments to complete the compilation of threat sources for

evaluation. Using this list, an analysis of threat source capability, intent, and targeting is completed for threat sources where an adversary such as a hacker is involved. Threat sources such as floods that do not involve an adversary are rated for a range of effect on the organization.

Threat event evaluation.

After threat sources are compiled, the NIST methodology provides a step for the evaluation of threat events such as obtaining access to classified records. NIST (2012) methodology states that threat events should be rated in terms of their relevance to an organization. Relevance rankings include N/A, Possible, Predicted, Anticipated, Expected, and Confirmed. A threat event is considered more relevant if a threat event is associated with a confirmed organizational incident or a source of reliable authority.

In the Med-A risk assessment, threat sources and threat events were analyzed and rated in a combinational format since the relevance of a threat event was connected to a threat source. Likewise, the capability, intent, and targeting of a threat source required consideration of a threat event. This combinatorial approach provided grounded discussion with the ability to focus on particular example scenarios such as unsecured patient insurance claims documentation with PII and PHI detail.

Likelihood of initiation / adverse events.

Threat events were evaluated for likelihood to take place using one of two options. Threat events that involved a threat actor such as hacker of disgruntled employee were analyzed using a likelihood of initiation metric (NIST, 2012). Likelihood of initiation reflects the probability that a

threat actor will carry out a threat event. Options range from not likely to highly likely. A second option for where a threat event does not involve an individual rates the likelihood of a threat's occurrence.

Threat events were also assessed for likelihood of causing an adverse impact. This metric addressed the probability that a threat could contribute to an adverse loss or other consequence. Based on a threat event's likelihood to take place and potential for adverse impacts, a final combined likelihood was calculated for each threat event.

Freund and Jones (2016) indicate that a deficiency of the NIST risk framework is that the likelihood of an adverse event cannot exceed the likelihood of a threat event. For example, if a hacker has a low likelihood of compromising an EHR system which could have a very high chance of causing an adverse impact, then the overall likelihood of moderate is not consistent with a low probability hacking event. While Freund and Jones recommend adjusting the NIST overall likelihood determination scale which is observed in Appendix H, the Med-A clinic risk analysis used NISTs scales without revision. Through discussion of risk scenarios such as a severe earthquake which is a low probability event, it was determined that the NIST scales acceptably rated overall risk.

Level of Impact

The likelihood of impact is an evaluation of the outcomes from a successfully exploited vulnerability (Valacich & Schneider, 2016). Establishing a consistent approach to impact assessment requires the consideration of how an incident will affect the confidentiality, integrity and availability of information. Impact should address loss or damage such as "fire destroyed

paper files". If extreme impacts such as the destruction of all paper file exist, these scenario should be respectfully addressed rather than downgraded for risk mitigation (Freund & Jones, 2015).

Vulnerability Assessment

Vulnerabilities and predisposing conditions are weaknesses in an organization's information systems, policies, procedures, or controls and are specific to an asset or set of assets (Valacich & Schneider, 2016; NIST, 2012). Vulnerabilities are classified according to: a) hardware; b) software; c) network; d) personnel; and e) organization (Vacca, 2013). Predisposing conditions are pre-existing conditions within an organization that could influence the impact of successful threat event (NIST, 2012). An example predisposing condition is a building in an earthquake zone that lacks retrofitting protections for earthquakes.

NIST (2012) indicates that the complexity of business operations and information systems may result in addressing vulnerabilities at a more general level with respect to size, scope, and type. For example, a business' overall viability could be vulnerable to a severe earthquake if the business stores all assets in a single location. Effectiveness of considering more generalized vulnerabilities requires compartmentalizing vulnerabilities with respect to threat events and their impacts.

Healthcare-related vulnerabilities.

Healthcare infrastructure is particularly challenging for balance due to the complexity of systems and likely sources of threats. Healthcare systems employ a breadth of mature and modern technology to provide services. However, healthcare data breach events are likely to stem from

simplistic causes such as theft or bypassing weak authentication protocols (Mohammed, Mariani, & Mohammed, 2015). Insufficient system controls or lack of executively implemented security procedures may to increased vulnerabilities.

Vulnerability evaluation.

NIST (2012) vulnerability identification and analysis begins with determining potential vulnerabilities based on relevance, severity, and predisposing conditions. A set of vulnerabilities is compiled based on review of an organization's information systems, policies, and procedures and through the use of collective taxonomies of vulnerabilities such as The Open Web Application Security Project (OWASP)'s top ten vulnerabilities for web applications (OWASP, 2010). Another valuable source of vulnerability research is the National Vulnerability Database and Common Vulnerability Scoring System that is maintained by NIST (2012). Vulnerabilities are compiled into a list for severity rating. Predisposing conditions are also rated for their pervasiveness across an organization.

Risk Determination

Final overall likelihood determination.

The overall risk for a threat event and its impact are determined by the likelihood that a threat event successfully exploited a vulnerability and the resulting impact (NIST, 2012). This final metric is identified as the risk determination. NIST provides an assessment scale that was used for final risk determination, but NIST's guidance suggests that the provided risk determination scale be used as a guide. NIST contends that cases with higher-level impact may not have an explicit upper round of impact. In addition, NIST recommends review of moderate impact assignments for

complex scenarios where a higher-level impact may exist for cumulative moderate impacts.

Ranking and final assessment.

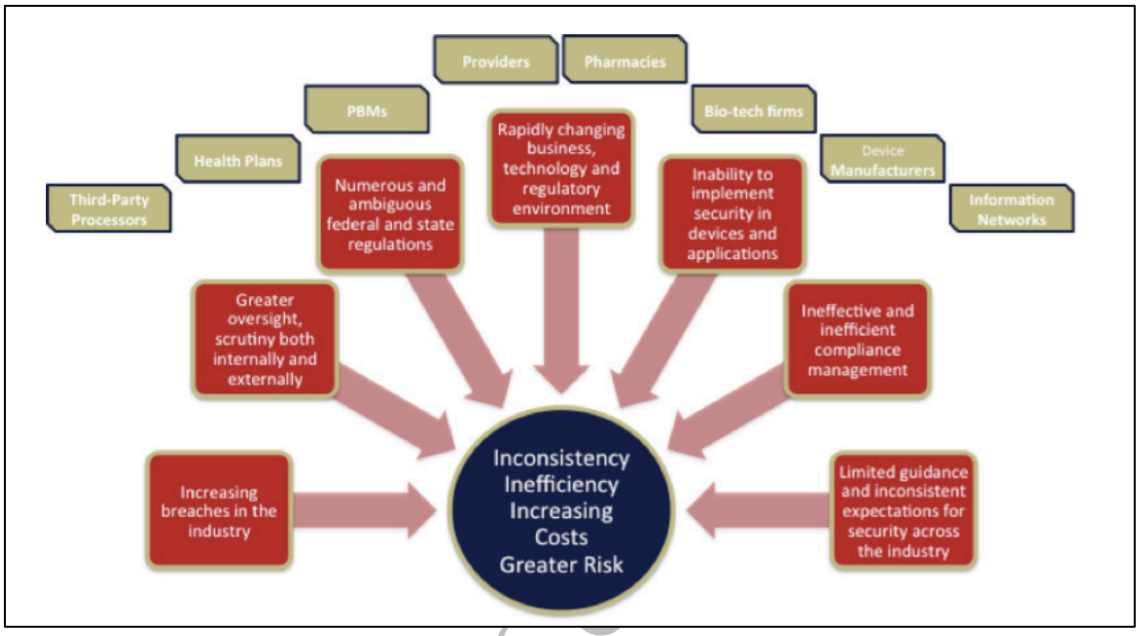
A final ranking exercise was completed after risk determination to address potential complexities associated with overall impacts and combinational impacts that result from a single successfully executed threat event.

Countermeasures

A countermeasure is a safeguard that is targeted to remediate a specific threat (Bayne, 2002). Countermeasures are recommended as a means to correct vulnerabilities and reduce the potential attack surface that could be exploited by threat actors (UcedaVelez & Morana, 2015). Traditional countermeasures are broadly recommended by information security research groups such as NIST and government entities such as CMS OCR (Landoll & Landoll, 2005; NIST, 2012).

Appendix B

HITRUST Overview of Risk Factors in Healthcare



Appendix C

Human and Non-human Threat Sources

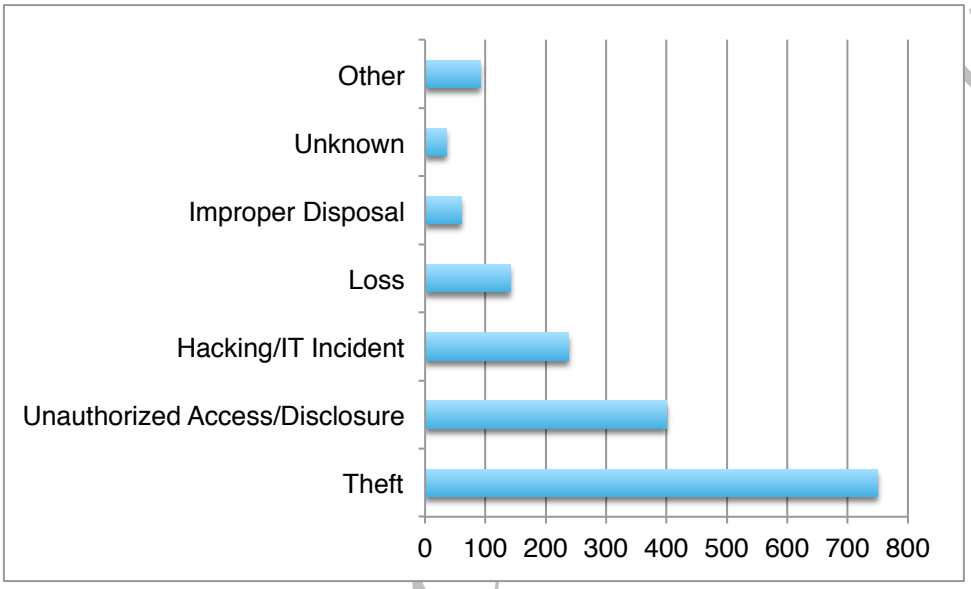
Human	Non-Human
• Hackers • Theft (electronically and physically) • Non-technical staff (financial/accounting) • Accidental • Inadequately trained IT staff • Backup operators • Technicians, Electricians	• Floods • Lightning strikes • Plumbing • Viruses • Fire • Electrical • Air (dust) • Heat control

Examples of human and non-human threat sources. Reprinted from *An Overview Threat and Risk Assessment* (p. 6), by J. Bayne, 2002, Bethesda, MD: SANS Institute. Reprinted with permission.

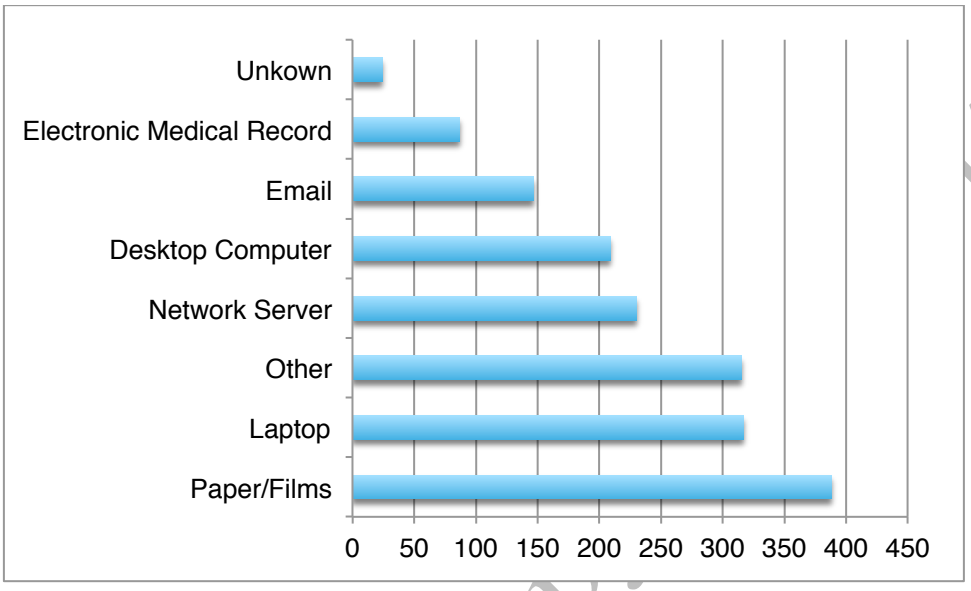
Appendix D

Types of Healthcare Data Breaches with Greater than 500 Individuals

as Reported to CMS OCR (2016)



Media Associated with Healthcare Data Breaches of Greater than 500 Individuals as Reported to CMS OCR (2016)



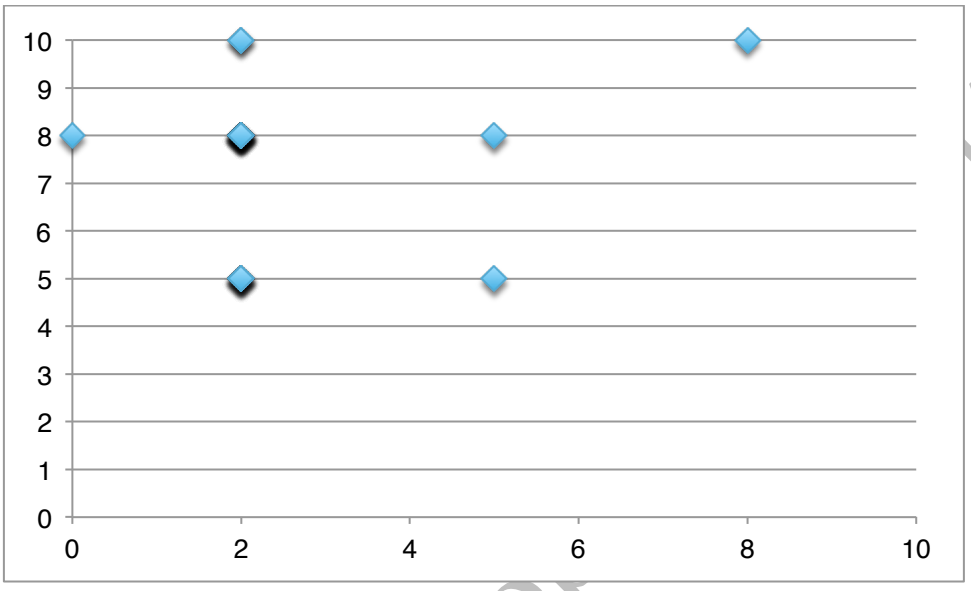
Appendix E

High Severity Ranked Vulnerabilities

Final Adjusted Top Vulnerabilities Based on a High Severity Rating	
Vulnerability Source	Vulnerability
Employees	Copy and transport patient data to external devices. External device such as a laptop containing patient or clinical data.
Employees	Removing or disabling security tools
Employees	Connecting personal devices to company networks
Employees	Writing down passwords and sensitive data
Technology	Internet browsers
IT Management	Improper waste disposal (e.g, paper records)
Partners and Suppliers	Hardware failure such as hard drive failure (by IT vendor)
Partners and Suppliers	Software failure such as failure of EMR software storing patient data in unsecured file system folders (by IT vendor)

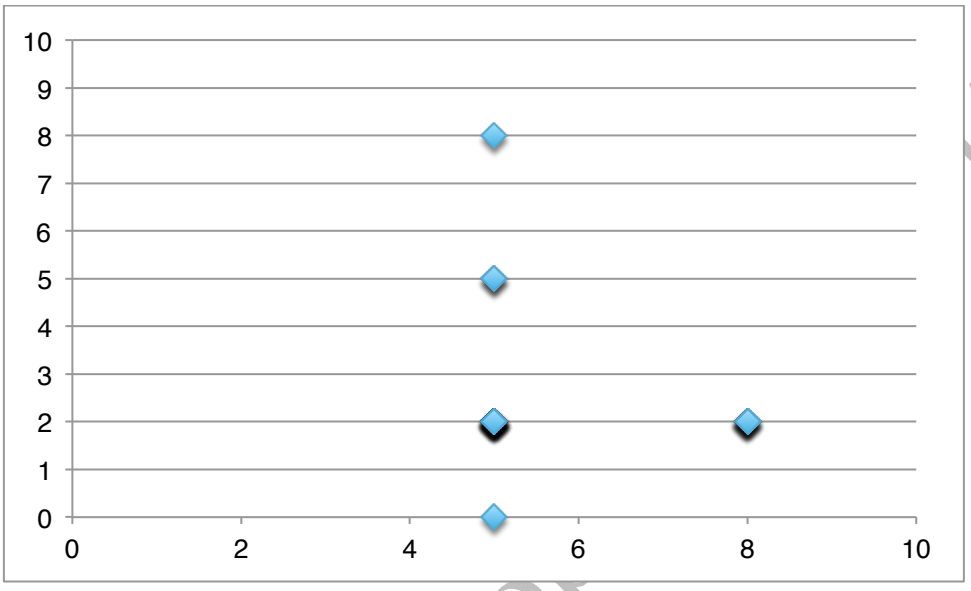
Appendix F

Likelihood Initiation / Occurrence versus Likelihood Adverse Events

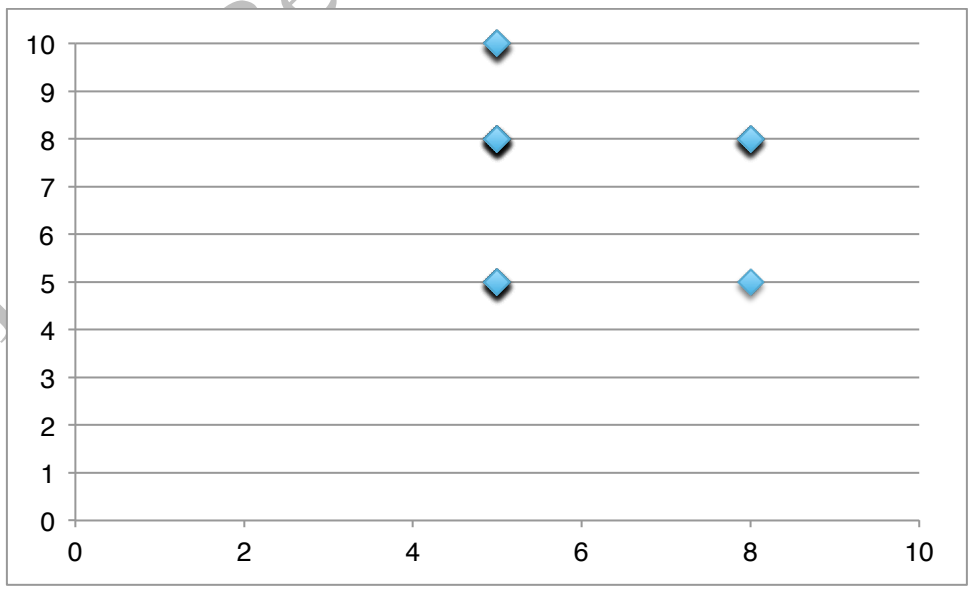


Appendix G

Likelihood Initiation / Occurrence versus Level of Impact



Likelihood Adverse Events versus Level of Impact



Appendix H

Risk Assessment Results Adjusted with Ranking

Top Unadjusted Risks Based on Determination and Ranking						
Ranking	**Threat Source**	**Threat Event Source of Information**	**Likelihood of Threat Event Initiation or Occurrence**	**Likelihood of Threat Event Resulting in Adverse Impacts**	**Level of Impact**	**Risk Determination**
1	Outside attacker	Obtain sensitive information via exfiltration.	Low	High	High	High
1	Former employee	Obtain sensitive information via exfiltration.	Low	High	High	High
1	Current employee -- intentional	Obtain sensitive information via exfiltration.	Low	High	High	High
2	Outside attacker	Cause deterioration/destruction of critical information system components and functions.	Low	High	High	High
3	Outside attacker	Insert targeted malware into organizational information systems and information system components.	Low	Very High	Moderate	High
4	Outside attacker	Deliver targeted malware for control of internal systems and exfiltration of data.	Low	Very High	Moderate	High
5	Outside attacker	Craft spear phishing attacks.	High	Very High	Moderate	High
6	Current and Past Employees	Theft - Taking data out of the office (paper, mobile phones, laptops)	Low	High	Moderate	Moderate
7	Current and Past Employees	Theft of clinical research	Low	High	Moderate	Moderate

9	Envirnonmental	Earthquake - Severe (non-adversarial)	Very Low	High	Moderate	Moderate
10	Envirnonmental	InfrastructureFailure/Outage ElectricalPower (non-adversarial)	Low	Moderate	Moderate	Moderate
11	Hacker	Exfiltration of clinical research	Low	High	Moderate	Moderate
12	Envirnonmental	InfrastructureFailure/Outage Telecommunications (non-adversarial)	Low	Moderate	Moderate	Moderate
13	Current employee	Viewing patient records outside of assigned patient workload.	Moderate	Moderate	Moderate	Moderate
14	Outside attacker	Extortion of money for release of patient data	Moderate	High	Moderate	Moderate
15	Outside attacker	Cause disclosure of critical and/or sensitive information by authorized users.	Low	High	Moderate	Moderate
16	Natural event	Fire at primary facility (non-adversarial)	Low	Moderate	Moderate	Moderate
17	Current employee	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement). (non-adversarial)	Low	High	Moderate	Moderate
18	Outside attacker	Obtain sensitive information through network sniffing of external networks (e.g., Starbucks)	Low	Moderate	Moderate	Moderate
19	External consultant	Compromise organizational information systems to facilitate exfiltration of data/information.	Low	Moderate	High	Moderate

Final Adjustment Top Ten Risks Based on Determination and Ranking			
Ranking	Threat Source(s)	Threat Event Source of Information	Risk Determination
1	Outside attacker / Former employee / Business consultant	Obtain sensitive information via exfiltration (not device).	High
2	Outside attacker	Cause deterioration/destruction of critical information system components and functions.	High
3	Outside attacker	Deliver targeted malware for control of internal systems and exfiltration of data.	High
4	Outside attacker	Craft spear phishing attacks.	High
5	Current / Past employees	Theft - Taking data out of the office (paper, mobile phones, laptops)	Moderate
6	Current / Past employees	Theft of clinical research	Moderate
7	Environmental	Earthquake - Severe (non-adversarial)	Moderate
8	Current employee	Viewing patient records outside of assigned patient workload.	Moderate
9	Environmental	InfrastructureFailure/Outage ElectricalPower (non-adversarial)	Moderate
10	Outside attacker	Exfiltration of clinical research	Moderate

Appendix I

NIST 800-30 RMF Overall Risk Likelihood Scale

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Security risk determination rating from NIST 800-30. Reprinted from *Guide to Conducting Risk Assessments*, by NIST, 2012, Department of Commerce. Reprinted with permission.