HEALTHCARE CASE: STANDARDS-BASED APPROACH TO CYBERSECURITY

Derek Bowdle
EN.695.601
November 28, 2022

Preface

The following paper will describe how Cyber-Physical Systems (CPS) can transform Dr. Jones Hypothetical Fairfax INOVA Hospital Transplant Center to maximize efficiency and economic benefits. First, the driving question will be summarized and reflected upon. Next, the NIST approach will be expounded and examined. Then, the NIST Seven Step Gap Analysis will be applied to the use case. Finally, the case is analyzed using the NIST Federal Cyber Security Approaches.

Table of Contents

Section 1: Question ….…….. 4
Section 2: Interpretation of Question ……..……..4
Section 3: Introduction……..……..6
Section 3.1: NIST Approach ……..6
3.1.1 NISTIR 8170 Figure 2: Three organization levels ……7
3.1.2 NISTIR 8170: Figure 2: Level 1: Organization ……..7
3.1.3 NISTIR 8170: Figure 2: Level 2: Mission/business processes ….. …7
3.1.4 NISTIR 8170: Figure 2: Level 3: System ……10
3.1.5 3.1.5 NIST SP 1500-202: Section 2.3.3 Optimize Cyber Physical System risk budget (safety, resilience, reliability, security, privacy) ……..10
Section 3.2: Inova Fairfax Transplant Center Use Case ……10
3.2.1 Inova Fairfax Transplant Center ……10
3.2.2 Hypothetical Inova Fairfax Transplant Center Use Case: RBAC “As-Is” ……..11
Section 4: NIST Seven Step Gap Analysis (NIST CSF Section 3.2: Establishing or Improving a Cybersecurity Program) ……13
Step 1: Prioritize and Scope ……13
Step 2: Orient ……13
Step 3: Create a Current Profile “As Is”: Use existing RBAC architecture……..13
Step 4: Conduct a Risk Assessment ……..15
Step 5: Create a Target Profile “To Be”: ABAC Architecture …….. …...16
Step 6: Determine, Analyze and Prioritize Gaps …….. 16
Step 7: Implement an Action Plan …….. 18
Section 5: Analysis …….. 18
5.1: Challenges of building and testing a candidate ABAC pilot program vs NISTIR 8170 Figure 2: Three organization levels: 1) Organization; 2) Mission/Business Processes; and 3) System: ABAC pilot program …… 18
Section 6: Conclusions …… 19
Section 7: References …… 20

List of Figures:

Figure 1: Federal Cybersecurity Approaches ……6
Figure 2: NIST Authentication Process Example ……12
Figure 3: Organizations Network Architecture ……..14

List of Tables:

Table 1: “As-Is” Access Control Table Mapping NIST Cybersecurity Framework to HIPAA ……..15
Figure 3: Zero Trust Access ……17
Figure 4: Zero Trust Logical Components ……17

Section 1: Question

The key question of this investigation is: using Cyber-Physical Systems (CPS), how can Dr. Jones Hypothetical Fairfax INOVA Hospital Transplant Center be converted in order to meet the needs of a modern economy? A CPS is defined as multiple smart systems which require the integrated use of physical and computational components, which comprise the overall engineered networks. These networks involve various "smart" application domains, such as smart manufacturing, transportation, energy, and healthcare. Therefore, the question at hand is how to take this hypothetical hospital's isolated domains, and maximize its economic potential by connecting each aspect of the entity's process through the application of CPS.[1]

Section 2: Interpretation of Question

The need for an investigation of this kind is imperative in order to meet the demands of a modern economy. In 2014, the National Institute of Standards and Technology (NIST) devised "Approaches for Federal Agencies to Use the Cybersecurity Framework" that detailed its vitality, and will therefore be used as a use case. This publication allowed experts to outline the attributes of CPS in a public forum, so that others may understand, develop and apply these systems to their own, which is what the present investigation will explore.

As previously mentioned, the overall goal is to remain economically competitive, and integrating networks would allow the hospital to do this, because innovative applications will not only be able to reach multiple domains, but also require and provide more detailed information. This data will enable stakeholders to make more informed decisions, thus reaping economic benefits to both the entity and to consumers. For example, the Internet of Things (IoT) involves the manufacturing domain, because it deals with the physical engineering of technologies. So, if each step of the manufacturing process were meticulously documented through a smart application as opposed to an unintegrated system, then it is easier to track what materials are being used, and perhaps more importantly what is not being used. Altogether, the introduction of a smart application could enhance the manufacturing process, so that there is an increased amount of accountability, and systems can be refined, improved and ultimately maximized. Taking this example one step further, the Industrial Internet allows materials, such as sensors, devices and computer applications to be interconnected. Instead of having machines operate independently of one another, the use of smart applications would maximize efficiency through automation, which would require less employees to manage the systems, and decreased time in producing actual products. In all, the manufacturing domain would benefit immensely from the introduction of a CPS.

In addition to the manufacturing domain, transportation allows medical materials to reach the final destination, the hospital. Smart applications provide an entirely transformative element of accountability that could potentially save lives. Tracking items from the time of departure, stops along the way, and final destination in the end allows

[1] NIST Special Publication 1500-201: Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0, June 2017. Figure 1: CPS Conceptual Model.

medical professionals to make more informed decisions for how to treat their patients. Furthermore, transportation could also extend to ambulances, in which the same benefits can occur, only in this case it would allow hospitals to communicate with those in transit, so that they could immediately treat patients as they arrive at the hospital. Smart applications could also be utilized when in transit as diagnostic and treatment tools, so when it comes to these technologies there is an immense amount of opportunity for innovation and growth with biotechnology. Hence, this further supports that implementing a CPS is especially aligned with the modern economy.

Energy is the foundation to the daily operations of a hospital, so the employment of a CPS through smart applications will not only support the modern economy, but also the well-being of all patients. Tracking energy usage could help the hospital plan for projected costs, and what to do in case of emergency. If the hospital were ever to not have access to energy then this could put numerous lives at stake. Therefore, digitizing all of the information using a CPS, so that the information is integrated into a network could allow the information to be controlled and addressed externally. In the modern economy, it may also be beneficial to investigate how to utilize alternative energies in not only the case of emergency, but also as a long term energy source in order to decrease impacts of global warming. In all, this can contribute to a modern economy because it supports both patients and medical professionals, and could also support other growing industries.

Lastly, healthcare services at the hospital would optimize economic benefits through the integration of smart applications. From connecting patients to doctors, to accessing physical medicinal supplies, to documenting each step of the process, having information interconnected through a centralized system is essential to the hospital's success. Having scheduling completed through an integrated network allows individuals to connect themselves with healthcare professionals, which is extremely cost efficient, and if they do need to speak with a healthcare professional directly, then having access to a centralized calendar system would make those connections seamless. In addition, similar to the manufacturing domain, utilizing an integrated system for tracking all medicinal supplies is also economically beneficial, because it keeps inventory as up to date as possible, and can track which supplies are most needed and can help with efficiency in both ordering, so they know what consumers require most.

In summary, the interpretation of this question is multifaceted, but ultimately provides compelling evidence that it is economically advantageous to administer a CPS. Smart applications offer an extra element of accountability for manufacturing, transportation, and energy so that information can be accounted for, tracked and the hospital can then use that information accordingly to better inform their practices. Healthcare from the individuals it serves to the products it is utilizing would also benefit immensely from having information shared through a network. In all, these will help to better serve people, and more efficiently use items, so that the hospital remains economically competitive, and will ultimately influence a plethora of economic domains in the worldwide economy. This will all be possible through drawing upon the framework of the NIST approach as a case study. The following sections will delve into the specific steps required to create a CPS, so that it transitions from Role Based Access Control (RBAC) to an Attribute Based Access Control (ABAC). In the end, this

will create an Electronic Healthcare Records (EHR) system, which meets the criteria for a CPS, requires smart applications, and will ultimately contribute greatly to the modern economy.

Section 3: Introduction

Section 3 explores the NIST Approach for cybersecurity, which is divided into an organizational, mission/business processes and systematic levels. The organization level establishes what cybersecurity policies to prioritize, and makes it understandable to all stakeholders involved. The mission/business processes have many components to it, as it deals with management, acquisitions, assessments, outcomes, structure and reporting systems. The final level summarizes all of the cybersecurity documents through a centralized document, so that it is not only clearly defined, but also aligned with the mission. The subsequent subsections will go into more detail about the aforementioned levels and components to create a holistic understanding of the recommended Federal Cybersecurity Approaches.

Section 3.1: NIST Approach

The NIST Approach recommends that the core of the Cybersecurity Framework involve a Risk Management Framework (RMF). That is, cybersecurity must take into consideration risk factors when devising a CPS. This is particularly pertinent, because CPS requires an interconnected network, and as established previously this helps tremendously with access to information, but also permits breach in privacy. Thus, it is essential to consider all risks at all levels of organization, which are described in the subsequent section.

Special Publication 800-37 Rev. 2 Levels				Cybersecurity Framework Components
	Level 1 Organization	**Integrate enterprise and cybersecurity risk management** by communicating with universally understood risk terms.	Core	
	Level 2 Mission/Business Processes	**Manage cybersecurity requirements** using a construct that enables integration and prioritization of requirements.	Profile(s)	
		Integrate and align cybersecurity and acquisition processes by relaying cybersecurity requirements and priorities in common and concise language.	Profile(s)	
		Evaluate organizational cybersecurity using a standardized and straightforward measurement scale and set of self-assessment criteria.	Implementation Tiers	
		Manage the cybersecurity program by determining which cybersecurity outcomes necessitate common controls and apportioning work and responsibility for those cybersecurity outcomes.	Profile(s)	
		Maintain a comprehensive understanding of cybersecurity risk using a standard organizing structure.	Core	
		Report cybersecurity risks using a universal and understandable structure.	Core	
	Level 3 System	**Inform the tailoring process** using a comprehensive reconciliation of cybersecurity requirements.	Profile(s)	

Figure 2: Federal Cybersecurity Approaches

Figure 1: Federal Cybersecurity Approaches

Source: NIST Special Publication 1500-201: Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0, June 2017. Figure 2: Federal Cybersecurity Approaches.

3.1.1 NISTIR 8170 Figure 2: Three organization levels

The three levels of organization outlined in the NIST report include: organization, mission/business process and system. First, the relationship between these three levels is a bilateral one, in which all risk considerations taken at the organization level are also assumed in levels two and three. The difference is the specificity where there is only a broad-based risk perspective at level one, but as the levels ascend they become more detailed and granular. Regardless of the level, there is communication and reporting at each level, and risk management is the core of each one.

3.1.2 NISTIR 8170: Figure 2: Level 1: Organization

The primary role of the organizational level is to identify potential cybersecurity risks, and have a method for assessing, mitigating and recovering from them if an error were to occur. In addition to cybersecurity, the organization would also cover anything concerning safety, finances, programs, acquisitions, supply chains, and privacy. Because the goal is to have the majority of this information stored in a smart application, and accessible through a centralized network, it is inevitably a cybersecurity issue, and thus must be considered at the organizational level. Cybersecurity is enforced through the enactment of policies, therefore at this level understanding risks using universal language is essential to prevent issues from arising, and having contingency plans if problems were to occur. Ultimately, the effectiveness at the organization level is only achieved when representatives such as agency stakeholders, and executive leadership from the entire enterprise are capable of identifying and prioritizing risk management factors, and this, again, is accomplished through developing common language and policies.

3.1.3 NISTIR 8170: Figure 2: Level 2: Mission/business processes

At the mission/business level the hospital must consider: cybersecurity requirements, alignment of cybersecurity and acquisition processes, organizational and management of cybersecurity, and a comprehensive understanding and reporting system for cybersecurity risks. Cybersecurity requirements include anything from insurance privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, to payment processes, such as the Payment Card

Industry Data Security Standard.[2] The organization, in this case a hospital, must be knowledgeable of cybersecurity requirements that apply to them, which involves an integration of their current cybersecurity measures with what is required by law. In all, identifying cybersecurity requirements ensures that the business level meets compliance, which can also lead to further efficiency and effectiveness. From a business' mission perspective, it can help identify priorities, and assess potential threats, which can facilitate the operationalization of cybersecurity activities.

After the cyber security requirements have been identified, the hospital must integrate and align cybersecurity and acquisition processes by relaying cybersecurity priorities in both common and concise language. This will ensure that regardless of what level of interface an employee interacts with, anyone affiliated with the hospital will not be in violation of any of the cybersecurity requirements. This common language is extended into contracts, this way there is documentation within written agreements, which can ultimately protect the hospital from cybersecurity threats. Similarly, offerors, which in the case of a hospital would be contractors and patients, would be permitted the same cybersecurity rights to protect themselves, so contracts would reflect language that offerors would like in the contracts as well. Lastly, in the case of a major IT acquisition federal agencies have the liberty to discern which entities to conduct business with organizations to ensure that their operations, products and services uphold minimum cybersecurity requirements. Because integrating and aligning cybersecurity systems including the acquisition processes is so involved, it includes but is not limited to the following stakeholders: Risk Executive (Function), Chief Information Officer (CIO), Senior Information Security Officer/Chief Information Security Officer (CISO), General Counsel, Contracting Office, mission/business owners, and stakeholders representing other risk management disciplines (e.g., finance, human resources, purchasing). In all, this involved process ensures that even when new offerors are contracted through the hospital that cybersecurity will be at the forefront of the acquisition process.

The next tier transitions into implementation, or what is required once contracts are put into action. The next aspect of the Mission/Business Processes is the evaluation of organizational cybersecurity using standards-based and straightforward measurement scales, and self-assessment criteria. For example, cybersecurity properties can be evaluated using a scale of 1 to 4: partial, risk-informed, repeatable, and adaptive, respectively. The overarching goal of the utilization of a scaled assessment, such as this one, is to ensure that the system is not only functional, but also repeatable in the future. Repeatability can extend into enterprise risk management, and outside

[2] “NCP - National Checklist Program Checklist Repository.” n.d. NCP. Accessed November 23, 2022. https://checklists.nist.gov/.

parties affiliated with the hospital. That is, in implementing the cybersecurity systems, repeatability allows the hospital to identify any areas of improvement, and the overall investments made in cybersecurity.

Once the cybersecurity system is implemented, it must be managed by having defined roles and responsibilities to execute the cybersecurity objectives. In order to be effective in this pursuit, units and individuals must be held accountable, and subsequently be rewarded when they perform adequately. This, in turn, will empower employees to fulfill their cybersecurity responsibilities, and always strive to do better. In assessing cybersecurity outcomes, it is also helpful to recognize the common and hybrid controls. This analysis of outcomes creates a better level of accountability, because the hospital can reassess if the defined roles are appropriate, or if the responsibilities should be redefined for business units and/or individuals. Ultimately, this is economically beneficial, because in consistently analyzing outcomes, the hospital can potentially save on significant resources once they have identified the common controls.

Next, the utilization of a standard organizing structure helps the hospital gain an in-depth understanding of cybersecurity risk. This is done through measuring, assessing, and reporting on different elements of cybersecurity risk. This comprehensive understanding prepares for a proactive versus reactive approach to cybersecurity, because in the process threats are evaluated, likelihood of threats are projected, and potential impacts are measured and as a result planned for.

Finally, cybersecurity risks must be reported using a universal and understandable structure. Standardized reporting ensures that everyone in the hospital is familiar with the same structure, and builds a culture of documenting any cybersecurity risks that may arise. Additionally, the operative word for this requirement is understandable, because if the reporting process is not straightforward, then not everyone will be able to report cybersecurity risks, so this is the key element of this requirement.

3.1.4 NISTIR 8170: Figure 2: Level 3: System

The last level of the Federal Cybersecurity Approaches is to systemically inform the tailoring process using a comprehensive reconciliation of cybersecurity requirements. This reconciliation should take the form of a document that summarizes not only the mission objectives, but also cybersecurity requirements, so that there is a structure an employee can reference as they consider cybersecurity.

3.1.5 NIST SP 1500-202: Section 2.3.3 Optimize Cyber Physical System risk budget (safety, resilience, reliability, security, privacy)

Furthermore, a CPS must be equipped to combat physical, cyber, and hybrid (cyber-physical) attacks, and this is done through a holistic approach. Attackers will often target one or more of these systems, so it is vital that CPS operators are knowledgeable about the way that these systems interact with one another. Consequently, this requires CPS operators to create algorithms, risk mitigation strategies and methods to detect attacks. In all of this, there is a holistic approach in which the CPS does not use discipline-specific silos, but rather assesses systems as they interact with one another.

CPS can involve physical, analog, and cyber elements, each of which are accounted for in the risk budget, but not necessarily in equal increments as each has their own respective limitations and risk factors involved. One of these factors includes security, which is both how the security operates, but also its reputational risks. It also takes into consideration errors that may occur that can impede safety and reliability, which also takes into account failure rates. Next, privacy speculates what to do with unwarranted disclosure rates. Last, resilience plans for recovery rates. In summary, when analyzing risks, each of these components is taken into consideration on a holistic level, because if attackers have access to one, then they may impede on others.[3]

3.2: Inova Fairfax Transplant Center Use Case

3.2.1 Inova Fairfax Transplant Center

The Inova Fairfax Transplant Center is an organ transplant center located in Northern Virginia. They pride themselves as one of the nation's best hospitals and provide what they call “full scope” inpatient and outpatient services for a large range of transplant patients. In addition to

[3]Barrett, Matt, Victoria Yan Pillitteri, Jon Boyens, Stephen Quinn, Greg Witte, and Larry Feldman. 2020. “NISTIR 8170 Approaches for Federal Agencies to Use the Cybersecurity Framework.” National Institute of Standards and Technology, (March). https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf.

prioritizing high quality care they also prioritize reducing cost where possible so their care is as cost effective as possible.[4]

In order to provide such outstanding care Inova provides its employees access to a wide range of services through various online services. A remote smart scheduling service, charts, radiology, emergency alerts, a dedicated Intranet containing employee policies, departmental information, employee newsletters, and announcements, and a VPN[5] provide employees access to everything without having to be within the hospital.[6] To manage this they have their terms and conditions of use detailing what they are responsible for when it comes to these online resources and explicitly informing users that the material viewed through them might be sensitive.[7] Additionally they have a mobile device management policy that outlines privacy, device support, security, and liabilities which users must sign and acknowledge before use.[8]

3.2.2 Hypothetical Inova Fairfax Transplant Center Use Case: RBAC "As-Is"

For our hypothetical Inova Fairfax Transplant Center use case we have three silos and four user groups. The silos are broken down into the Radiology Department, Dr. Jones Transplant Center, and the VPN. The four user groups in order of least to most restricted are doctors, nurses, administrators, and patients. With these, the current access control system works by creating credentials for each user then based on which user group the user belongs to the system grants access. For example, both doctors and nurses have access to a patient's chart but only the doctor would have access to the patient's scans. This is also extended to read and write permissions; doctors, nurses, admin, and patients could view appointments but only administrators could write or change them. This is slightly expanded by having a separate radiology system in which doctors in the transplant center have access to information in radiology yet doctors in radiology do not have access to information in the transplant center. The last silo to discuss is the VPN that provides doctors, nurses, and admin the ability to access sensitive documents. When using the VPN access corresponds to the permissions that the user has when accessing either the radiology or transplant center systems though this would be done so by connecting through the VPN.

---

[4]"Inova Transplant Services." 2022. Inova Transplant Services. https://www.inova.org/our-services/inova-transplant-services.
[5]"Employee Access and Resources." 2022. Inova. https://www.inova.org/for-employees.
[6]"Employee Access and Resources." 2022. Inova. https://www.inova.org/for-employees.
[7]"Web Policies." 2022. Inova. https://www.inova.org/about-inova/web-policies.
[8]"The Mobile Device Management Policy." 2015. Inova. https://www.inova.org/sites/default/files/mobile-device-mgmt.pdf.

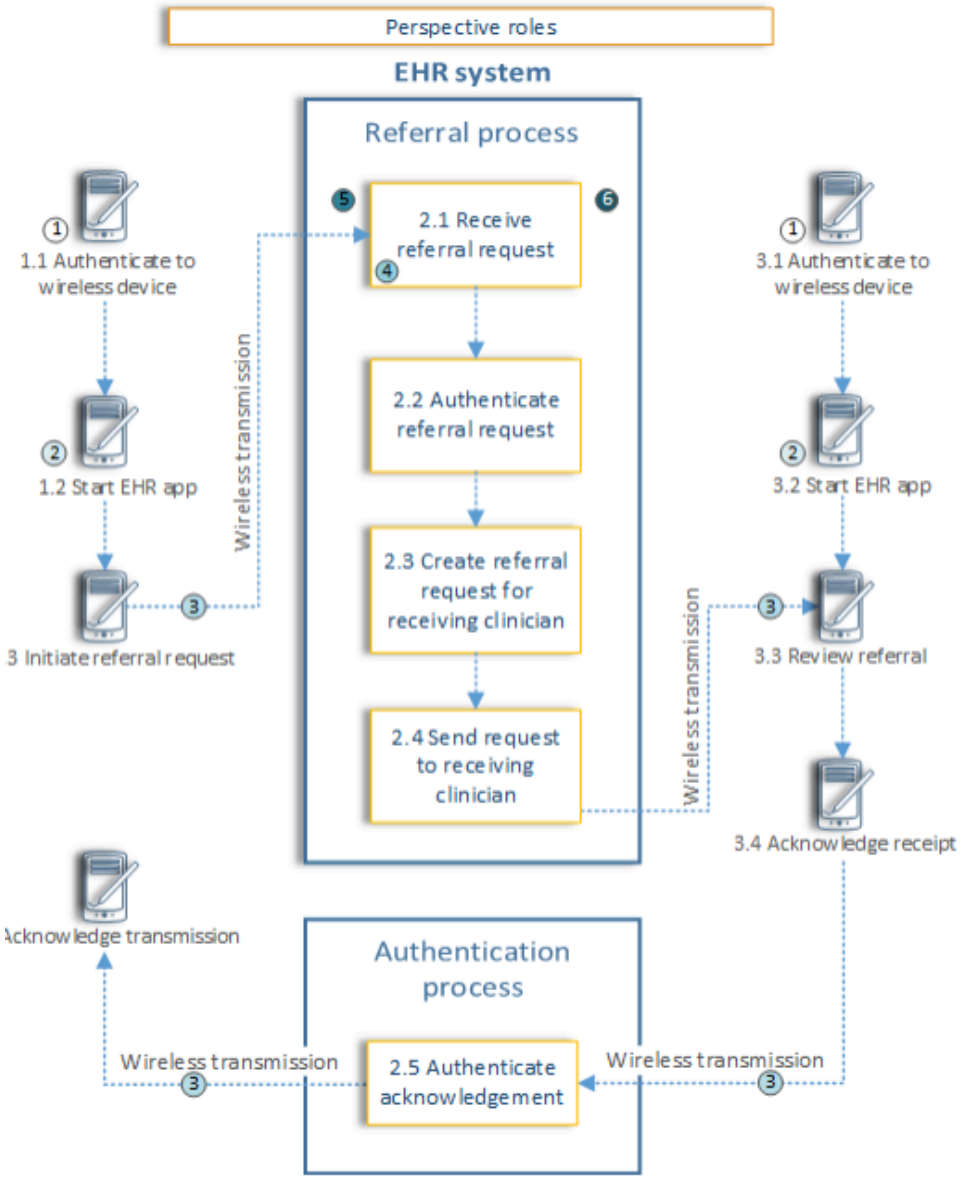

Figure 2: NIST authentication process example
Source: NIST SP 1800-1B Draft: Securing Electronic Health Records on Mobile Devices: Approach, Architecture, and Security Characteristics, July 2018, Figure 3-1; and NIST: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, Appendix A, Table 2

The above figure details how the current RBAC system would authenticate and set roles using the wireless system. Let's say that an admin is onboarding a new patient, they would have the patient authenticate using their wireless device, start the EHR app then initiate the referral request. The admin would then authenticate on their own device, start the app then review the request and acknowledge it if it is valid. From there the patient would acknowledge that they received it to complete the process.

Section 4: NIST Seven Step Gap Analysis (NIST CSF Section 3.2: Establishing or Improving a Cybersecurity Program)

We will be using the Seven Step Gap Analysis provided by the National Institute of Standards and Technology (NIST) in their Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 to determine the best course of action for the Hypothetical transition of Inova Fairfax Transplant Center's access control system from Role-Based Access Control (RBAC) to an Attribute-Based Access Control (ABAC).

Step 1: Prioritize and Scope

The top priority of the Inova Fairfax Transplant Center is to keep patient information and records as private as possible. Access must be not only lawful but also with purpose. This includes preventing unlawful, unintentional, or unmerited access by not only malicious actors but also by legitimately authorized users. The scope of this analysis will be restricted to systems and assets related to access control. It will however include not only accessible through the transplant center but also through the Radiology department as well as remote access to the various systems.

Step 2: Orient

The analysis extends to any and all systems related to access control. This includes any and all authentication systems as well as any authentication hardware such as PKI cards or RSA tokens. Any servers holding user credentials and relevant authentication information are also extended to. All of the operations of the access control system must also comply with the multitude of HIPAA rules and requirements. It is also clear that the best approach to unacceptable access would be to avoid it wherever feasibly possible.

Step 3: Create a Current Profile "As Is": Use existing RBAC architecture

The current Electronic Health Record (EHR) system uses a constrained Role-Based Access Control (RBAC) system. This system operates within three different silos: The Radiology Department, Dr. Jones Transplant Center, and the VPN. The following figure is an example of what the network architecture of the system looks like.

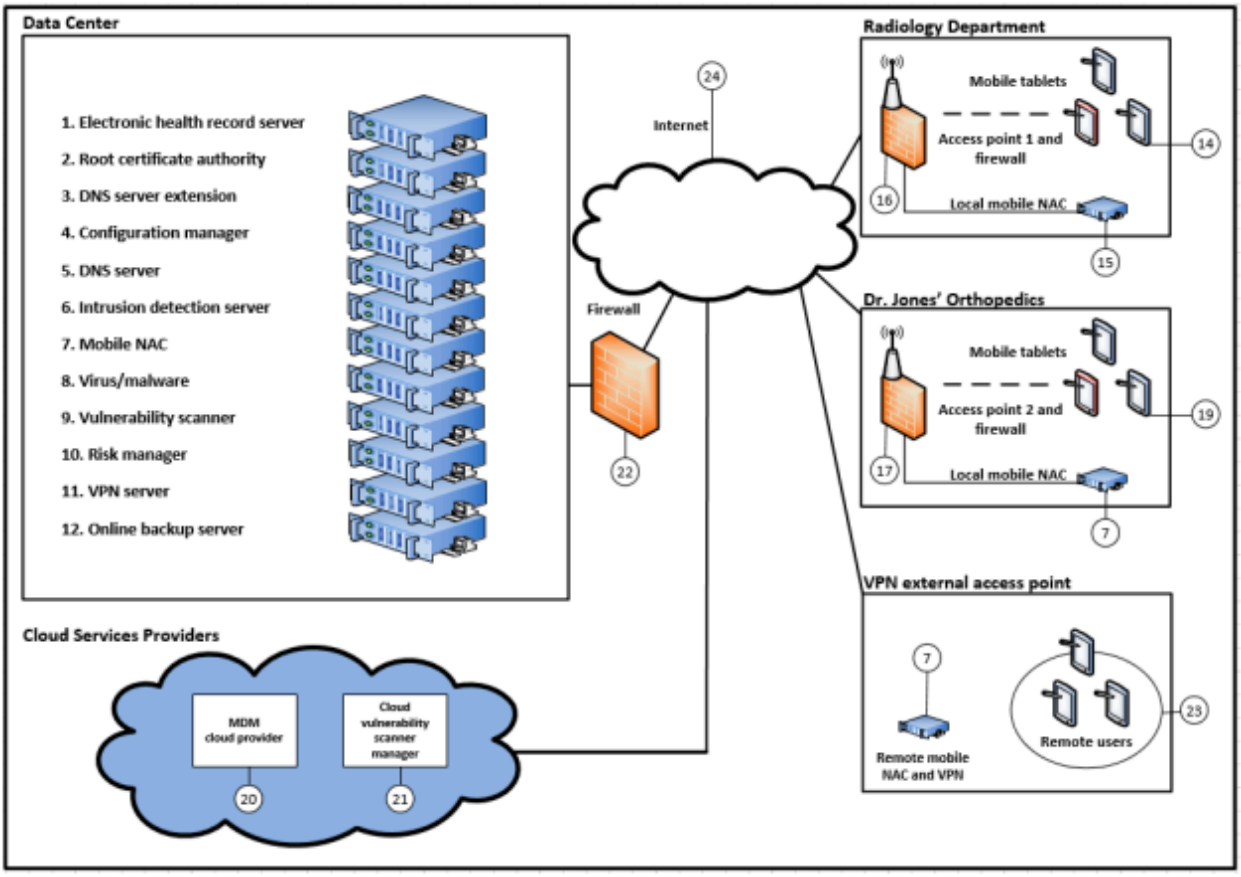

Figure 3: Organizations Network Architecture
Source: "NIST SPECIAL PUBLICATION 1800-1B - Securing Electronic Health Records on Mobile Devices." 2018. NCCoE. https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-ehr-nist-sp1800-1b.pdf.

In this example, Dr. Jones' Orthopedics would be replaced with the Inova Fairfax Transplant Center. All silos have their own firewall, including the data center, and they are all connected via the internet, including any external cloud service providers. Both the radiology department and transplant center offer connections via wireless access points and local connections.

Security Characteristics	NIST Cybersecurity Framework Function	NIST Cybersecurity Framework Category	CSF Subcategory	HIPAA Rule Description	HIPAA Security Rule
access control	Protect (PR)	Access Control (PR.AC)	PR.AC-1, PR.AC-3, PR.AC-4	Technical safeguards	45 CFR § 164.312 (a)
device integrity	Protect (PR)	Access	PR.AC-3	Administrative	45 CFR §

		Control (PR.AC)		safeguards, Technical safeguards	164.308 (a)(5)(ii)(B), 164.312 (c)
person or entity authentication	Protect (PR)	Access Control (PR.AC)	PR.AC-1, PR.AC-3, PR.AC-4	Administrative safeguards, Technical safeguards	45 CFR § 164.308 (a)(5)(ii)(D), 164.312 (a)(2)(i), 164.312 (d),
transmission security	Protect (PR)	Access Control (PR.AC)	PR.AC-3	Technical safeguards	45 CFR § 164.312 (e)

Table 1: "As-Is" Access Control Table mapping NIST Cybersecurity Framework to HIPAA

Source: "Securing Health Records on Mobile Devices." 2015. National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-ehr-nist-sp1800-1d-draft.pdf.

This table shows the security characteristics connected to access control and maps them to the associated HIPPA Rules. Below are the full descriptions for the CSF Subcategories.

PR.AC-1: Identities and credentials are managed for authorized devices and users
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate[9]

Step 4: Conduct a Risk Assessment

The fundamental risk with the current access control system is that if a hostile actor accesses a single user's credentials they can pull all data that the user has permission to access. With one instance of access, a large volume of data is extractable, especially for specific users. For the current system, Doctors would have by far the most access to sensitive patient information, therefore if access is gained through a transplant center doctors identity a hostile actor could

[9]"Securing Health Records on Mobile Devices." 2015. National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-ehr-nist-sp1800-1d-draft.pdf.

extract information about many patients not only related to what was collected in the transplant center but also any radiology information as well as past records.

Any proposed changes to the current access control system needs to balance safety, security, reliability, resilience, and privacy while also prioritizing them in that order. It is important to note that safety is the number one priority, any modifications must not restrict legitimate access because restriction of critical information could lead to loss of life.

Step 5: Create a Target Profile “To Be”: ABAC Architecture

We assume that the current RBAC architecture is HIPAA compliant; any addition would only be to strengthen already existing rules. For example, 45 CRF § 164.312 (a)(1) states “Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).”[10] which suggests that only those that have been granted access can have access which is something that can always be improved upon. All access control systems have this as an aim though some are more successful than others.

The new ABAC architecture should incorporate resource attributes such as creation date, resource owner and sensitivity level as well as environmental attributes such as time, location, and threat level to determine access. These attributes would work together with pre-existing user attributes which already limit access by principles of least privilege and separation of duties. For example if a request to access a large amount of patients' social security numbers is made from an administrator's account from a remote location that request should be denied due to the sensitivity level of the resource, the volume of data, and the location where the request was made. These rules need to be defined to restrict access wherever possible while also making sure to never restrict in a way that could result in restriction of access to a legitimate actor to information that could result in harm. Something like information related to patients' allergies to medication should not be overly restricted, yet due to it being sensitive information requests should be monitored for suspicious requests.

Step 6: Determine, Analyze and Prioritize Gaps

The largest gap in the current access control system is its ability to use the resource and environmental attributes to restrict user access. Once that ability is gained all that must be done is to set the rules that govern permissions and set up some kind of zero trust monitoring.

[10]“45 CFR § 164.312 - Technical safeguards. | Electronic Code of Federal Regulations (e-CFR) | US Law | LII / Legal Information Institute.” 2013. Law.Cornell.Edu. https://www.law.cornell.edu/cfr/text/45/164.312.

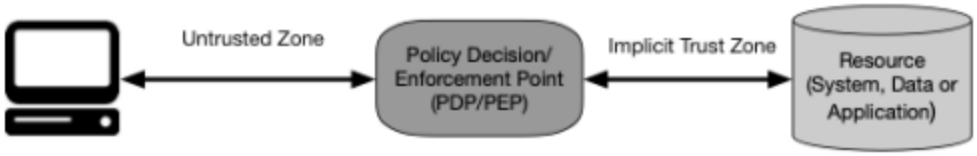

Figure 1: Zero Trust Access

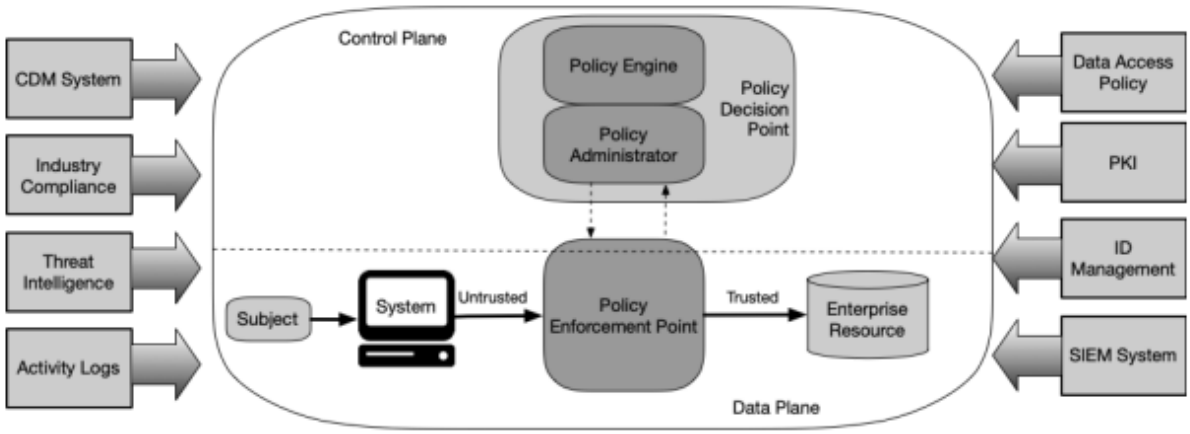

Figure 2: Core Zero Trust Logical Components

Figure 3: Zero Trust Access
Figure 4: Zero Trust Logical Components

Source: “Zero Trust Architecture.” NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Any system implemented must operate on a zero trust architecture as shown above in the two figures. The key difference between the previous architecture and the new suggested zero trust architecture is that once a user uses their credentials to authenticate their login to the system they would now continue to be considered a possible hostile actor and also continue to be monitored and possibly restricted based on their actions.

A possible cost effective solution is to implement a third party identity and access management solution as well as a third party Zero trust monitoring provider. ManageEngine AD360 provides both identity and access management solutions that would be capable of implementing zero trust access control and replace the current VPN.[11] It also provides zero trust monitoring.

Step 7: Implement an Action Plan

[11]“One-stop solution for all your identity and access management needs.” 2022. Manage Engine. https://www.manageengine.com/active-directory-360/tp/identity-and-access-management-solution.html?utm_source=eSecurityPlanet&utm_medium=tp_cpc&utm_campaign=ad360_zerotrust.

It is recommended that the Inova Fairfax Transplant Center integrates some kind of third party zero trust solution in order to transition its current role based access control system to an attribute based access control system. It is recommended to integrate the identity and access management solutions ManageEngine AD360 provides or something similar to upgrade the system. This will provide more secure access control while also enabling removal of its current VPN access. The trade off between increase in security and cost is very fair and should be seriously considered.

Section 5: Analysis

5.1: Challenges of building and testing a candidate ABAC pilot program vs NISTIR 8170 Figure 2: Three organization levels: 1) Organization; 2) Mission/Business Processes; and 3) System: ABAC pilot program

By implementing a third party identity and access management solution we can not only save the hospital money by not having to make major modifications to their existing system but also save any burden placed on their hospital through the act of having to transition to a new system. Operations should be fairly uninterrupted and we should see no impact to maintaining operations or patient safety levels. There should also be no difficulty in communicating the changes to the whole of the organization due to most changes being imperceptible to users using the system. The one major change would be the replacement of the VPN which would require a decent amount of communication and guidance to transition users to the new system. Rolling out and testing the new permissions would also need to be done very carefully, most likely in a way where permission rules are created then tested on user data without restricting access in the case that tested rules are too restrictive. This testing would then result in a ABAC pilot program in which a subset of selected or volunteer candidates could test the new authentication system and report and issues before being rolled out and mandated for the entire hospital.

Section 6: Conclusions

By using the guidance lent by NIST in their Seven Step Gap Analysis and Federal Cyber Security Approaches Inova Fairfax Transplant Center could greatly improve their security in a cost effective way by transitioning their current access control system from Role-Based Access Control (RBAC) to an Attribute-Based Access Control (ABAC). With support of leadership the organization as a whole would improve by decreasing the likelihood of a data breach while not impacting operations or putting patients at risk. The mission and process would also benefit by making them more HIPAA compliant while also not being interrupted. The system as a whole will benefit by adding new tools that can continue to be used and refined enabling IT professionals to create a system that will likely be capable of handling the current needs as well as any future needs.

Section 7: References

Barrett, Matt, Victoria Yan Pillitteri, Jon Boyens, Stephen Quinn, Greg Witte, and Larry Feldman. 2020. “NISTIR 8170 Approaches for Federal Agencies to Use the Cybersecurity Framework.” *National Institute of Standards and Technology*, (March). https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf.

“Employee Access and Resources.” 2022. Inova. https://www.inova.org/for-employees.

“45 CFR § 164.312 - Technical safeguards. | Electronic Code of Federal Regulations (e-CFR) | US Law | LII / Legal Information Institute.” 2013. Law.Cornell.Edu. https://www.law.cornell.edu/cfr/text/45/164.312.

“Inova Transplant Services.” 2022. Inova Transplant Services. https://www.inova.org/our-services/inova-transplant-services.

Kindervag, John. 2020. “Zero Trust Architecture.” NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

“The Mobile Device Management Policy.” 2015. Inova. https://www.inova.org/sites/default/files/mobile-device-mgmt.pdf.

“NCP - National Checklist Program Checklist Repository.” n.d. NCP. Accessed November 23, 2022. https://checklists.nist.gov/.

“NIST SPECIAL PUBLICATION 1800-1B - Securing Electronic Health Records on Mobile Devices.” 2018. NCCoE. https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-ehr-nist-sp1800-1b.pdf.

“One-stop solution for all your identity and access management needs.” 2022. Manage Engine.

https://www.manageengine.com/active-directory-360/tp/identity-and-access-management-solution.html?utm_source=eSecurityPlanet&utm_medium=tp_cpc&utm_campaign=ad360_zerotrust.

“Remote and Extended Access.” 2022. Inova. https://www.inova.org/for-employees/remote-extended-access.

“Securing Health Records on Mobile Devices.” 2015. National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-ehr-nist-sp1800-1d-draft.pdf.

“Web Policies.” 2022. Inova. https://www.inova.org/about-inova/web-policies.