AIRA
AMERICAN IMMUNIZATION REGISTRY ASSOCIATION
Immunization Information Systems for a New Era




Security Guidance

Considerations for Immunization Information Systems

June 2017

Executive Summary

The purpose of this document is to explore the various issues that impact IIS security and provide guidance on industry standards and best practices for addressing common security concerns. This document is a companion document to the guidance on "Confidentiality and Privacy Considerations for IIS"[1] released in October 2016 and is intended to complement the primary guidelines provided under the CDC IIS Functional Standards and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Content was informed through a review of relevant legal requirements for IIS security, best practice guidance for electronic health system security, and security standards as defined by the National Institute of Standards and Technology (NIST). Interviews were conducted with industry experts to clarify and enhance the discussion on various elements of system and electronic data security.

The material in this document has been customized specifically for use by IIS managers, IIS staff, and immunization program managers (hereby referred to collectively as IIS administrators). Relevant information has been distilled into guiding security principles, recommendations, and supporting resources. This document is intended as a guide to assist IIS administrators in engaging their IT staff and vendors in conversations to ensure that an IIS is protected by appropriate security measures in accordance with industry best practices. Each section includes a set of questions titled "Conversation Starters" to help facilitate these discussions.

The first step in evaluating IIS security and/or developing appropriate IIS security plans and policies is to perform a **Risk Assessment**. Risk Assessment is generally comprised of a **Risk Analysis** to identify all security threats and vulnerabilities that affect the IIS and **Risk Management** that encompasses all the administrative and technical safeguards and controls implemented to address the risks identified through the Risk Analysis. This document focuses on a variety of common IIS threats and the controls that can be put in place to help an IIS **prevent** a security incident, **detect** a breach or attack, and **respond** to and **recover** from a security event.

The following list represents actionable items that IIS administrators can perform immediately to begin improving IIS security:

- **Compile and review documented policies and procedures** that relate to IIS security.
- **Identify the agency's Security Officer, IT Administrator, and other key players** to begin the conversations about IIS security policies and practices.
- **Conduct a Risk Assessment** of the IIS through a tabletop exercise with key players.
- **Identify known gaps and establish a plan** to implement appropriate security controls.
- **Review IIS configurations and feature functionality** to ensure they align with current security standards.
- **Request copies of existing Business Associate Agreements (BAAs) and Service Level Agreements (SLAs) related to the hosting and support** of the IIS and review these documents for security protections that are and are not covered under these agreements.

[1] http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf

IIS administrators should take an active role in understanding and guiding IIS security practices. Threats, technologies, and security standards evolve rapidly, and IIS staff should not assume that current security measures remain adequate or appropriate. Security management should be an active and ongoing practice that is incorporated into all areas of IIS routine operations. As threats and vulnerabilities are identified, IIS administrators should be prepared to **accept**, **prevent**, **eliminate**, or **transfer** the risk. Documentation should be created and reviewed/updated on a routine basis, and policies and procedures should be strengthened as needed to support evolving security strategies. Security tools, procedures, and plans should be regularly tested through tabletops and/or active functional tests to ensure that the IIS is properly positioned to manage a physical or cyber attack.

Disclaimer: The information contained in this document represents a point-in-time review of current industry standards and best practices. Readers should be aware that standards and practices evolve over time. This guide should not be interpreted as a mandatory requirements or standards document. It contains a set of recommended guidelines that can be implemented for improving the security of immunization information systems. The information in this document is not legal advice. Each IIS should contact appropriate individuals within their own agency who are responsible for the interpretation and implementation of federal, state, local, and territorial laws as they develop new and/or update existing security policies.

Table of Contents

Acknowledgments

The American Immunization Registry Association (AIRA) would like to acknowledge and thank the following individuals and organizations for their support and assistance with this important project:

- The primary researcher and writer on this project: **Danielle Reader-Jolley**, Public Health Consultant
- The security and technical experts who contributed their expertise through discussion and document review:
  - **Roderick Duff**, Information System Security Officer, NCIRD, Centers for Disease Control and Prevention
  - **Francesca Lanier**, Chief Information Security Officer and Chief Privacy Officer, Utah Department of Health
  - **Quan Le**, Registry Program Manager, Louisiana Department of Health (Office of Public Health Immunization)
  - **Steve Murchie**, CEO, Envision Technology Partners
  - **Matthew Scholl**, Chief, Computer Security Division, NIST
  - **Anurag Shankar**, Senior Security Analyst, Indiana University (Center for Applied Cybersecurity Research, Pervasive Technology Institute)
  - **Shenny Sheth**, Information Security Manager, Texas Children's Hospital
  - **Gary Wheeler**, IIS Executive and Strategist, DXC Technology
  - Scientific Technologies Corporation
    - **Brandy Altstadter**
    - **Cory Hopple**
    - **Joseph Jaganathan**
    - **Azure Spanier**
    - **Marty Ulrich**
- The AIRA Board of Directors who provided input at various stages of the effort and/or reviewed and provided comments on the final guide:
  - President: **Michelle Hood**, Nebraska Department of Health and Human Services
  - President-Elect: **Kim Salisbury-Keith**, Rhode Island Department of Health
  - Immediate Past President: **Mary Woinarowicz**, North Dakota Department of Health
  - Secretary: **Jenne McKibben**, Oregon Immunization Program
  - Treasurer: **Belinda Baker**, Washington State Immunization Information System
  - Directors
    - **Bridget Ahrens**, Vermont Immunization Registry
    - **Brandy Altstadter**, Scientific Technologies Corporation
    - **Kevin Dombkowski**, University of Michigan, Child Health Evaluation and Research Unit
    - **Brittany Ersery**, Kansas Department of Health and Environment
    - **Baskar Krishnamoorthy**, Florida Department of Health IIS
    - **Quan Le**, Louisiana Immunization Program
    - **David McCormick**, Indiana State Department of Health
    - **Megan Meldrum**, New York State Immunization Information System

- The AIRA Staff who contributed to this document's development:
  - **Nathan Bunker**, Senior Technical Project Manager
  - **Rebecca Coyle**, Executive Director
  - **Mary Beth Kurilo**, Policy and Planning Director
  - **Nichole Lambrecht**, Senior Project Manager
  - **Eric Larson**, Senior Technical Project Manager
- Individuals who provided feedback during the external review process:
  - **Noam Arzt**, President, HLN Consulting, LLC
  - **Janet Fath**, Operations Team Lead, IIS Support Branch, NCIRD, CDC
  - **Elaine Lowery**, Public Health Consultant
  - **Craig Newman**, Health Research Analyst, Northrop Grumman/IIS Support Branch, NCIRD, CDC
  - **Laura Pabst**, Deputy Branch Chief, IIS Support Branch, NCIRD, CDC
  - **Veronica Rodriguez**, Data Manager, Immunization Program, Puerto Rico Health Department

Chapter 1. Introduction

Modern day news is frequented by headlines about security breaches and cyber attacks that can have significant personal, political, and financial ramifications:

Major Security Breaches Found in Google and Yahoo Email Services *(May 2016, Huffington Post)*[2]

Ransomware Expected to Dominate in 2017 *(January 2017, Computer Weekly)*[3]

Hack May Have Exposed Info on 390,000 People Tied to Homeland Security *(June 2015, NBC News)*[4]

DDoS Attack That Disrupted Internet Was Largest of Its Kind in History *(October 2016, The Guardian)*[5]

Hack of Democrats' Accounts Was Wider Than Believed *(August 2016, The New York Times)*[6]

Top 5 Healthcare Data Breaches in 2016 Not From Hacking *(March 2016, Health IT Security)*[7]

For health-specific incidents, the U.S. Department of Health and Human Services (DHHS), Office of Civil Rights (OCR) maintains the HIPAA Breach Portal[8] that documents all "Breaches Affecting 500 or More Individuals" reportable under HIPAA. The database contains the details of over 1,800 incidents reported from 2009 to present.

The purpose of this document is to explore the various issues that impact IIS security and provide guidance on best practices for addressing common security concerns. This document is a companion document to the guidance on "Confidentiality and Privacy Considerations for IIS"[9] released in October 2016. While the companion document focuses on maintaining "the privacy of individuals whose information is contained in IIS and the confidentiality of information disclosed to and by IIS," this document focuses on the security of IIS, specifically the administrative, physical, technical, and organizational safeguards designed to protect the IIS against unwarranted disclosure, modification, or destruction. Both documents complement the primary guidelines provided under the CDC IIS Functional Standards.

There are a substantial number of resources available that provide security guidance and detail on security standards for electronic systems. This large volume of resources can quickly become overwhelming. The material in this document has been customized specifically for use by IIS managers, IIS staff, and immunization program managers (hereby referred to collectively as IIS administrators). Relevant information has been distilled into guiding security principles, recommendations, and supporting resources. This document is intended as a guide to assist IIS administrators in engaging their IT staff and vendors in conversations to ensure that an IIS is protected by appropriate security measures in accordance with industry best practices. Each section includes a set of questions titled "Conversation Starters" to help facilitate these discussions.

While some IIS security aspects may be overseen by internal IT, external vendor staff, or other contracted third-party services, the entity defined as the "owner/operator" of the application is ultimately responsible for ensuring that the IIS is protected by appropriate security measures. This level of accountability may vary somewhat depending on how a jurisdiction has implemented its IIS. Typically, the legal responsibility will reside at the agency level (e.g., Department of Health), while the operational responsibility resides with the IIS Program itself.

[2] http://www.huffingtonpost.com/entry/major-security-breaches-found-in-google-and-yahoo-email-services_us_5729f450e4b016f378942950

[3] http://www.computerweekly.com/news/450410530/Ransomware-expected-to-dominate-in-2017

[4] http://www.nbcnews.com/tech/security/hack-may-have-exposed-info-390-000-people-tied-homeland-n376011

[5] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[6] https://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?_r=0

[7] http://healthitsecurity.com/news/top-5-healthcare-data-breaches-in-2016-not-from-hacking

[8] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[9] http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf

The content of this document was informed through a review of relevant legal requirements for IIS security, best practice guidance for electronic health system security, and security standards as defined by the National Institute of Standards and Technology (NIST). Interviews were conducted with industry experts to clarify and enhance the discussion on various elements of system and electronic data security. A list of interviewed security experts is included in the Acknowledgments.

Disclaimer: The information contained in this document represents a point-in-time review of current industry standards and best practices. Readers should be aware that standards and practices evolve over time. This guide should not be interpreted as a mandatory requirements or standards document. It contains a set of recommended guidelines that can be implemented for improving the security of immunization information systems. The information in this document is not legal advice. Each IIS should contact appropriate individuals within their own agency who are responsible for the interpretation and implementation of federal, state, local, and territorial laws as they develop new and/or update existing security policies.

Chapter 2. Data Security Regulations and Standards

Three primary resources were leveraged to inform the regulatory guidance and/or best practice considerations for ensuring or improving the security of IIS described in this document:

- CDC IIS Functional Standards 2018-2022
- HIPAA Privacy, Security and Breach Notification Rules
- NIST Special Publications

The following sections provide more detail on these initiatives.

CDC IIS Functional Standards

The Immunization Information System (IIS) Functional Standards were recently updated for 2018–2022[10] through a collaboration of the Centers for Disease Control and Prevention (CDC) Immunization Information Systems Support Branch (IISSB) and IIS stakeholders. The updated Functional Standards reflect the functionality an IIS should strive to attain to fully support immunization program operations and stakeholder immunization-related goals through 2022.

There are two core standards under "Essential Infrastructure Standards" that apply directly to IIS security policies and practices (FS 5.0 and FS 6.0). The various components of these core standards have been cross-referenced to the relevant sections of this document.

5.0 The IIS implements comprehensive account management policies consistent with industry security standards.

- 5.1 The IIS has a comprehensive written account management security policy or policies that are consistent with industry standards and reviewed and approved by the appropriate state or local authority. (Section: Numerous Sections)
- 5.2 The IIS requires unique log-in credentials for every IIS user who accesses the IIS through the user interface. (Section: User/Account Management)
- 5.3 The IIS ensures that each authorized site or information system (i.e., health information exchange) has unique credentials for electronic data exchange. (Section: User/Account Management)
- 5.4 The IIS establishes defined user roles and grants access to each individual user based on his or her role. (Section: User/Account Management)
- 5.5 The IIS creates and stores audit information, including the date, time, and the IIS user or site taking the action, when individual-level data in an IIS record are created, viewed, or modified. (Sections: User/Account Management and IIS Audit Logging)
- 5.6 The IIS identifies and inactivates user and site accounts when they are no longer active and/or no longer authorized to access the IIS. (Section: User/Account Management)

6.0 The IIS is physically and digitally secured in accordance with industry standards for protected health information, security, encryption, uptime, and disaster recovery.

- 6.1 The IIS has a comprehensive written physical and digital security policy or policies that are consistent with industry standards and are reviewed and approved by the appropriate state or local authority. (Section: Numerous Sections)
- 6.2 The IIS assures that demographic and vaccination information and authentication credentials are encrypted while in transit and while at rest. (Section: Data Protections/Encryption)
- 6.3 The IIS has written and implemented service-level agreements between the program, the entity providing information technology support, and other contractors as appropriate. (Section: Numerous Sections)

[10] https://www.cdc.gov/vaccines/programs/iis/func-stds.html

6.4 The IIS establishes backup and recovery plans identifying the required equipment, procedures, and the maximum allowable downtime for recovery from adverse security events and disasters. (Sections: Contingency Planning and Data/Database Backup Procedures and Restoration)

6.5 The IIS assures data and supporting software are backed up per a written policy and schedule. (Section: Data/Database Backup Procedures and Restoration)

6.6 The IIS assures that the system recovery and backup processes are tested and validated regularly. (Sections: Contingency Planning and Data/Database Backup Procedures and Restoration)

6.7 The IIS assures that the hardware and/or data center are physically and digitally secure. (Section: Facility, Workforce and Contracted Security Considerations)

6.8 The IIS assures that the hardware and/or data center have backup power. (Section: Facility, Workforce and Contracted Security Considerations)

6.9 The IIS has an identified point of contact for IIS security. (Section: Risk Assessment)

6.10 The IIS assures employees and business associates who will be administering or accessing the IIS data or infrastructure are familiar with applicable security policies and procedures. (Section: Facility, Workforce and Contracted Security Considerations)

6.11 The IIS assures that a risk analysis is performed on a regular basis. (Sections: Risk Assessment and Security Maintenance Routines)

HIPAA Privacy, Security and Breach Notification Rules

The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards that form a baseline for health information privacy and security protections. While only Covered Entities (CEs) and their Business Associates (BAs) are required by law to comply with HIPAA, all IIS can benefit from the adoption and implementation of HIPAA privacy and security practices.

> *The Health Insurance Portability and Accountability Act (HIPAA) provides stringent guidance for the protection of Personally-Identifiable Information (PII) and Protected Health Information (PHI). Although IIS are commonly recognized as Public Health entities and may not be strictly covered under HIPAA, the responsibility for strict confidentiality, privacy and security remain fundamental to IIS operations.*[11]

The **HIPAA Privacy Rule** addresses the protection of individual privacy and individually identifiable health information. The Privacy Rule is described at length in the "Confidentiality and Privacy Considerations for IIS" document.

The **HIPAA Security Rule** establishes national standards for the security of electronic PHI (ePHI). The HIPAA Security Rule is intended to cover "all ePHI created, received, maintained or transmitted by an organization," and where possible, entities should "implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards."[12] The general concepts and guidelines detailed in the Security Rule provide standards of practice that can, and should, be applied to the extent possible for the protection of all IIS and the data held therein.

This document will provide guidance on specific security topics that support the application of the overarching HIPAA Security "Standards" with special attention to items identified as "Required" in Subpart C – Security Standards for the Protection of Electronic Protected Health Information.[13] See Appendix E for a quick reference HIPAA security matrix.

[11] http://www.cdc.gov/vaccines/programs/iis/func-stds.pdf

[12] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

[13] https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164-subpartC.pdf

The following resources can be leveraged by any IIS program to assess for security risks and implement appropriate security protections. These resources are presented in a format that can be easily and efficiently reviewed by the reader:

- Security Rule Guidance Material[14]
- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (NIST 800-66 r1)[15]
- ONC Health IT Guide to Privacy and Security of Electronic Health Information, specifically Ch. 4 and Ch. 6 (focuses predominantly on EHRs, but the application of security policies and technical considerations can be directly employed by the IIS)[16]

The **HIPAA Breach Notification Rule** provides a definition of what constitutes a breach, guidance on unsecured PHI, breach notification requirements, and instructions for submitting a notification. This information can be found on the HIPAA Breach Notification website.[17]

The HIPAA Breach Notification Rule requires CEs and BAs to provide notification following a breach of *unsecured* PHI. Unsecured PHI is defined as any PHI "that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology…"[18] PHI is considered "secured" if it has been encrypted in accordance with industry best practices such as those defined by NIST. PHI may also be considered "secured" if the media on which the PHI was stored or recorded has been destroyed in such a way that the data cannot otherwise be reconstructed.

Security breaches have the potential to destroy public trust about the safety of their protected health information, but could also have financial or personal safety ramifications depending on how compromised data is used. While many IIS are not considered CEs under HIPAA, if patient data has been knowingly or potentially compromised, the IIS may still have a legal or ethical obligation to notify patients of the nature and extent of the security event. IIS not governed by HIPAA are encouraged to familiarize themselves with state or local laws, regulations, and policies regarding notification requirements and procedures.

The DHHS Office for Civil Rights (OCR) is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules. This includes conducting HIPAA complaint investigations, compliance reviews, and audits. *Note: If you are unsure about whether your IIS is a HIPAA Covered Entity, please consult with your agency's designated Privacy/Security Officer.*

NIST Special Publications

NIST is the National Institute of Standards and Technology, an agency under the U.S. Department of Commerce. Federal agencies are required by law to comply with NIST security standards. NIST Special Publication Series 800 specifically addresses computer security. SP 800 contains approximately 188 documents (and historical references) that provide extremely detailed and explicit guidance on all elements related to securing electronic systems and data.

While only federal agencies are required to follow NIST guidelines, these guidelines represent the current industry standards and should be applied by IIS as best practices for securing ePHI to the extent possible. Several specific NIST SP 800 documents will be referenced throughout this document, but the complete list of all computer security standards documentation can be found on the NIST Special Publications website.[19]

NIST has also developed a HIPAA Security Rule Toolkit to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. The Toolkit can be downloaded for Windows, Linux or Apple Mac OS at the following website: https://scap.nist.gov/hipaa.

[14] http://www.hhs.gov/hipaa/for-professionals/security/guidance/

[15] http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf

[16] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

[17] https://www.hhs.gov/hipaa/for-professionals/breach-notification/

[18] http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

[19] http://csrc.nist.gov/publications/PubsSPs.html

Chapter 3. Risk Assessment

The first step in evaluating IIS security and/or developing an overall IIS Security Plan is to perform a Risk Assessment. Risk Assessment is generally comprised of two components: Risk Analysis and Risk Management. **Risk Analysis** should be viewed as an ongoing activity for IIS administrators and should be performed on a regular basis (preferably annually) to account for evolving threats and new technologies. **Risk Management** encompasses all the administrative and technical safeguards and controls implemented to address known security threats and vulnerabilities identified through the Risk Analysis.

Each jurisdiction should have a designated Security Officer who manages the implementation and enforcement of security policies and activities for the organization. *Note: If you need assistance identifying this resource, the National Association of State Chief Information Officers (NASCIO) published the "State Cybersecurity Resource Guide"*[20] *that provides the primary contact for each state.* It is likely that the Security Plan for the entire organization has been documented using the NIST Risk Management Framework (RMF)[21] or a similar tool/process (e.g., Federal Acquisition Regulation (FAR) RMF or Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)). IIS administrators should identify their designated Security Officer and determine to what extent the IIS has been assessed or documented as part of the larger RMF. IIS administrators should also leverage the Security Officer to help guide or advise any IIS-specific risk assessment activities. Other key players that may have a role in IIS Risk Assessment have been defined in Appendix A. Glossary of Terms.

When it comes to Risk Assessment, an organization may opt to conduct its own risk assessment or to hire a certified health information professional to perform the analysis and recommend controls. Only an internal asset and someone close to the IIS will fully understand the system, the players, the workflows and data flows. In this case, an internal risk assessment will provide a more robust foundation for the overall security solution. An external review typically utilizes a checklist template that can be leveraged for any system. These external reviews can help "certify" that the basic components of a security solution have been addressed. External reviews can be very expensive and possibly cost-prohibitive, but a program may want to make this type of investment every few years (e.g., every five years) to ensure that the system continues to comply with basic industry standards. *Note: HIPAA-covered entities are required to participate in a formal HIPAA Risk Analysis to ensure that all HIPAA requirements have been addressed.*

Regardless of how an organization chooses to proceed with its Risk Assessment, there are several tools to help facilitate this process. For more information on Risk Analysis and Risk Management, the following resources may be helpful to the IIS community:

- HIPAA Security Series (topic 6) – Basics of Risk Analysis and Risk Management[22]
- NIST Guide for Conducting Risk Assessments (NIST 800-30 r1)[23]
- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171 r1)[24] (represents a simplified version of NIST 800-53)
- OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule[25]
- Security Risk Assessment Tool[26] (downloadable tool created by ONC, OCR and OGC to help guide organizations through the risk assessment process)

IIS administrators should never assume that IIS security has been adequately addressed. Simply because the IIS resides within a state or hosted environment or because it is subject to jurisdictional IT policies/procedures does

[20] https://nascio.org/Publications/ArtMID/485/ArticleID/435/State-Cybersecurity-Resource-Guide

[21] http://csrc.nist.gov/groups/SMA/fisma/framework.html

[22] http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

[23] http://csrc.nist.gov/publications/PubsSPs.html#SP 800

[24] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[25] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

[26] https://www.healthit.gov/providers-professionals/security-risk-assessment

not ensure that IIS security has been properly accounted for. As the "owner/operator" of the IIS and the data contained therein, IIS Programs and Departments of Health (or similar) have an obligation to protect ePHI through active security management.

Programmatically, IIS staff tend to focus only on the IIS application itself but need to expand that focus to include the entire data lifecycle (how data is collected, captured, stored, accessed, used, and destroyed). Documentation is critical, and a proper risk assessment should include full documentation of all systems, applications, data, and processes. This section will describe some primary considerations for IIS administrators and useful resources for performing Risk Assessment activities.

Risk Analysis

The first step in security planning is to perform a systematic Risk Analysis to identify potential security weaknesses. This analysis must be unique to each individual IIS and involves a custom review of all the people, workflows, data flows, and supporting processes involved with the IIS. This includes documenting all the various types of ePHI that the IIS creates, receives, maintains, and transmits, and then assessing all the human, technical, and environmental threats and vulnerabilities to that system and the related ePHI.

Some potential risks to IIS security may include:

- Inappropriate or unauthorized access, disclosure, modification, or destruction of e-PHI
- Ineffective/unenforced/non-existent/outdated policies, procedures, standards or guidelines
- Incorrectly implemented or configured system protections
- Cyber attacks (malicious software, network and computer based attacks, denial of service, hackers)
- Inaccurate data entry, inadvertent deletion, or malicious data entry/deletion
- Use of remote access and/or portable storage devices
- System failure, theft, vandalism, fire, natural disaster

Appendix F contains some additional examples of possible IIS security threats and vulnerabilities. These examples are intended to generate discussion and get IIS administrators thinking about the strategies they could implement to mitigate these risks. The examples included in the appendix are not intended to take the place of a customized IIS review using proven Risk Assessment tools/processes. To better understand the environment of current and evolving threats, readers are encouraged to periodically research "common cyber security threats." For example, in November 2016, McAfee produced a report titled "McAfee Labs 2017 Threats Predictions," which provides a comprehensive overview of current and emerging threats to cyber security.[27]

Once all IIS processes have been documented and threats/vulnerabilities have been identified, the next step is to assign a risk rating to each threat (high, medium, low). This can be determined by assessing the likelihood of threat occurrence and the potential impact should the threat occur. IIS administrators should then focus on prioritizing high-risk threat points before working through those categorized as medium or low.

[27] https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

Risk Management

Risk Management encompasses all the administrative and technical safeguards implemented to address the security threats and vulnerabilities identified through the Risk Analysis process. The first step of Risk Management is to review each security vulnerability that has been identified and determine whether the program will Accept, Prevent, Eliminate, or Transfer that risk.

- **Accepting** the risk means that the program is willing to accept the likelihood that the threat will occur along with any potential impact it may have on the IIS. An example includes providing usernames and passwords to prospective users without performing full background checks to verify identity and/or criminal history. In some cases, a written justification for why the IIS is willing to accept the risk may be needed.
- **Preventing/Mitigating** the risk includes any administrative, technical, and/or physical controls implemented by the IIS to protect against known threats to whatever extent possible. Most of this document will focus on the various control measures that can be implemented by IIS to address known risks.
- **Eliminating** the risk means removing the threat altogether. An example includes the practice of collecting and storing specific high-risk data fields, such as SSN (even last four digits) and/or mother's maiden name. In this example, the risk can be eliminated by removing these fields from the IIS entirely and changing the policies/practices around the collection of this information. *Note: This statement is not intended to conflict with guidance on CDC-endorsed data elements but, rather, to encourage discussion about weighing risk and benefit when it comes to collecting, storing, and securing high-risk/high-value data elements.*
- **Transferring** the risk means that the risk is transferred to and assumed by an external entity. An example includes the current trend to outsource hosting activities to an IIS vendor or leveraging virtual/cloud-based server environments. In this case, the host may assume responsibility for several basic security elements. The terms of these relationships are typically described in Business Associates Agreements (BAA) and/or Service Level Agreements (SLA).

The next step is to establish the appropriate strategies/measures to mitigate or remove the identified threats and vulnerabilities. This can be accomplished by first assessing currently implemented security measures and determining whether they are appropriate, adequate, and/or properly configured. Any remaining gaps should be acknowledged and provisioned with proper policies, procedures, or technologies to address the identified risks.

Risk management solutions should be implemented using a layered approach whenever possible or appropriate. For instance, the network layer provides the first line of defense against an external attack. This is followed by the host/application layer that prevents or detects both external and internal attacks. Finally, the "community" layer includes the people and processes to identify issues from the manual, human perspective.

Note: The ultimate test for any security solution is penetration testing, which involves hiring a certified expert to identify vulnerabilities in a security solution. These professional "hackers" attempt to expose weaknesses in the network, operating platform, IIS application, third-party support tools, and any other possible point of attack. A penetration test can be very expensive, so it may not be feasible for an IIS program to pursue this level of testing. It is still worthwhile for IIS to explore these services and the feasibility of having a test performed. In addition, some jurisdictions may conduct routine internal security scans (e.g., web application scans and network vulnerability scans) using commercially available tools such as those offered by Trustwave. IIS administrators should discuss internal scanning options and available tools with their IT counterparts.

Chapter 4. Administrative and Technical Security Controls

Once a Risk Analysis has been performed to identify all possible threats and vulnerabilities to the IIS, Risk Management is employed to determine how to best control for those risks. This chapter is dedicated to both the administrative and technical tools and processes that can be implemented to address IIS security. The various administrative and technical controls have been categorized into sub-chapters based on their primary function:

4.1 Prevention – Prevent or deter an attack on the IIS

4.2 Detection – Identify an attack in progress or after it has occurred

4.3 Response – Impede an attack and/or investigate the source and extent of the event

4.4 Recovery – Restore the IIS to normal operations and address exposed vulnerabilities

4.5 Routines – Address ongoing security maintenance activities

The following sections will provide guidance on the most common administrative and technical security measures that can be applied by an IIS. In addition to the material presented in this document, the DHHS Office for Civil Rights (OCR) produced a seven-part HIPAA Security Series. These documents are very readable and provide valuable guidance on implementing the various aspects of the HIPAA Security Rule. The documents on administrative, technical, physical, and organizational safeguards can be found by following the links below:

- HIPAA Security Series – Administrative Safeguards[28]
- HIPAA Security Series – Physical Safeguards[29]
- HIPAA Security Series – Technical Safeguards[30]
- HIPAA Security Series – Organizational, Policies and Procedures and Documentation Requirements[31]

Section 4.1: Prevention

The cornerstone of prevention is Risk Assessment as described in the previous section. Risk Assessment activities lay the groundwork for defining the administrative and technical controls to deter an event or attack to the extent possible. Most "prevention" strategies can be categorized as either network protections, data protections/encryption, or user management. Network infrastructure and data protections guard against external attacks, while user management guards against front-end or internal attacks. The following sections detail how these tools and methods can be applied to prevent or deter a security event.

Network and System Protections

Network and system protections predominately fall under the purview of IT and provide the first levels of security for defending the IIS against external attacks. External threats are constantly evolving and leveraging new technologies to identify vulnerabilities in networks, software, and data systems. These threats range from hobby hackers to elite international cybergangs and simple viruses to sophisticated software that hijacks data and holds it for ransom. While some of these attacks may be impossible to prevent, the IIS can certainly make an attack more difficult and/or make the IIS less visible or less interesting to potential attackers. This section describes the various layers of network and systems

[28] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es
[29] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf?language=es
[30] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es
[31] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf?language=es

protections from the outside in and provides suggestions on tools and configurations that should be explored or implemented by IIS administrators in conjunction with their IT counterparts.

- Perimeter controls – network firewalls, intrusion detection/prevention, DMZs, and VLANs
- System controls – operating system and web application firewalls, virus protection, email filters
- Maintenance controls – patch management, IT self-assessments

Network Firewalls:

Ports are the gateways that allow users to access the internet and ultimately the IIS. A network firewall will control which ports an organization wants to have open and available for access from external sources. The firewall sits right at the entry point of the internet service connection (e.g., the doorman at an upscale hotel). Open ports create vulnerabilities, so a properly configured firewall ensures that only specific ports with a specific purpose are allowed to be accessed by the internet at large. For IIS, this would include the web server port (typically port 443 for HTTPS).

Even by minimizing open ports, the web server port will continue to be subject to a significant amount of network and system traffic. Intrusion detection and prevention tools can help monitor and restrict undesirable traffic that exceeds expected thresholds. These tools may be included as part of the firewall, as part of a router that sits just inside of the firewall, or as a service installed on the actual server. These tools are described in detail in subsequent sections of this document, see Intrusion Detection and Alerting and Attack Mitigation.

Multilayer, next generation firewalls (in conjunction with intrusion detection/prevention tools) support the ability to block ports or specific IP addresses or restrict the application from interacting with various support tools (e.g., outbound email with SMTP or Google apps). While multilayer firewalls are mainstream in modern security strategies, it does not mean that IT consumers are taking full advantage of all the features these new firewalls offer. The IIS Risk Analysis can help determine what the proper firewall configurations should be.

Routers and router firmware can also become outdated. Router firmware can be updated in accordance with standing IT procedures and should be done on a routine basis. Router technology, like all technology, is always evolving. IT procedures should also include a schedule for replacement of security support tools after its durable life expectancy has been expended or as new technology standards are issued.

Demilitarized Zone (DMZ) vs. Virtual Local Area Networks (VLANs):

DMZs and VLANs allow an organization to segment its various networks and network assets. The primary difference is that DMZs represent a physical separation, whereas VLANs represent a virtual separation from the larger Local Area Network. For the IIS, a DMZ or VLAN would protect the IIS and IIS assets from the cascading effects of an attack on another system within the organization through compartmentalization. In the example above, you can get past the doorman, but you may be restricted to only the lobby or conference room A.

Operating System (OS) and Web Application Firewalls:

Where a network firewall protects against network attacks, an OS or Web Application Firewall protects against a specific targeted system attack. These tools typically reside on the actual web server. These firewalls can also be paired with intrusion detection and prevention tools for added security.

Virus Protection and Anti-Spyware:

Virus Protection and Anti-Spyware can be applied to servers and all user workstations and laptops. Like operating systems and IIS support software, the virus protection and anti-spyware tools should be routinely updated to protect against the most current security threats. These tools should be configured to perform regular scans for suspicious activity and alert users when activity is detected. Email filters can also be configured to identify and compartmentalize suspicious emails based on sender, content, or attachments.

Patch Management:

Just like software applications, operating systems and third-party support tools (e.g., Java, Adobe) also need to be updated with ongoing security updates and bug fixes. IT staff should be responsible for ensuring that operating systems and support software are up to date and properly maintained as part of the standard IT routines. Zero day vulnerabilities are problems or weaknesses in operating systems or software code that are identified and exploited by hackers before the product vendor

becomes aware of the issue. Once exposed, a vendor will often act quickly to resolve the issue and offer a patch to prevent further damage. For this reason, standing IT routines should account for all operating systems and third-party support tools that are subject to patching and versioning and should make sure that these tools are updated as soon as new patches or versions are released.

IT Self-Assessments:

While penetration testing may or may not be feasible for an IIS program to pursue, network vulnerability scans and web application scans (using tools like those available through Trustwave) can help identify common security risks so they can be appropriately addressed. IIS administrators should discuss these tools with their IT counterparts and include these scans as part of the annual IIS Risk Analysis. The results can then be used to identify any gaps and allow for the implementation or configuration of proper security controls.

Make the IIS Less Interesting:

A final high-level strategy is to make the IIS less interesting to external attackers. From a network perspective, this can be accomplished by using the network firewall to help "camouflage" the IIS by failing to respond to ping requests. If a hacker or sniffing tool is looking for a network, ignoring ping requests is one method to stay off the radar (e.g., a game of hide and seek). From a data perspective, IIS can make the data itself less interesting by removing fields like Social Security Number and mother's maiden name completely[32] or by using encryption strategies to make the data at rest and data in transit unreadable to an unauthorized user. These strategies are discussed in additional detail in the section on Risk Management and the following section on Data Protections/Encryption.

More information on network and system threats and protections can be found in the following documents:

- Guide to Malware Incident Prevention and Handling for Desktops and Laptops (NIST 800-83 r1)[33]
- McAfee Labs 2017 Threats Predictions[34]
- Fact Sheet: Ransomware and HIPAA[35]

Conversation Starters:

- ➔ What network security protections does the organization currently have in place to secure the IIS? Does the IIS operate in a DMZ or VLAN? Is the IIS protected by intrusion detection and intrusion prevention tools? Who is responsible for overseeing and maintaining network security?
- ➔ What system level security protections does the organization currently have in place to secure the IIS? Are firewalls enabled for the Operating System and/or Web Application? Is the server protected by an anti-virus software?
- ➔ Are there requirements for IIS users to maintain active anti-virus and anti-spyware software on their workstations or other tools used to access the IIS?
- ➔ What policies and procedures are in place to manage routine system patches for operating systems and third-party support tools? Is a log maintained to document when a patch has been applied and who performed the update?
- ➔ Has penetration testing, a network vulnerability scan, and/or a web application scan been performed in relation to IIS security? If so, when was the last test/scan performed and/or how often are these activities performed?

[32] *This statement is not intended to conflict with guidance on CDC endorsed data elements but, rather, to encourage further IIS community discussion about weighing risk and benefit when it comes to collecting, storing, and securing high-risk/high-value data elements.*

[33] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

[34] https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

[35] http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Data Protections/Encryption

Encryption is defined as "the process of converting information or data into a code to prevent unauthorized access" (Oxford English Dictionary). Decryption is the decoding or deciphering of encrypted data using an appropriate public or private key. A primary component of the HIPAA Breach Notification Rule is the differentiation between secure and unsecured ePHI. The Breach Notification Rule applies specifically to "*unsecured*" ePHI. Encrypting data is the primary mechanism to secure data at rest and data in transit from external attacks. There are three basic types of cryptography that may be employed by an IIS:

1. A block cipher can be used to perform full disk (server) and database encryption. Block ciphers allow data to be encrypted for storage but unencrypted for front-end users with appropriate system access permissions. For IIS, this means encryption of data at rest in the IIS database (e.g., patients, vaccinations, user details, logs, backups). Block ciphers are used primarily to protect the confidentiality of data.
2. Hash algorithms are used to generate an irreversible, fixed-length string of characters or numbers from data of any length. These algorithms are ideal for transforming super-sensitive data elements such as passwords or financial account numbers into a form that is secure and unreadable. For example, all passwords would be stored as a 32-character line of gibberish regardless of how many characters the password contained. Hash algorithms are also used to ensure data integrity by verifying that data at rest or in transit has not been changed, altered, or corrupted.
3. Hypertext Transfer Protocol (HTTP) paired with Transport Layer Security (TLS), also known as HTTPS, provides the primary mechanism for the encryption and transmission of messages between a submitting provider and the IIS – data in motion.

Most operating systems and database platforms (e.g., Microsoft, Oracle, Linux, SQL Server) include standard encryption tools. There should not be an additional cost to programs that are using one of these commercial product platforms unless they have implemented an algorithm that is not an included feature. There may, however, be a cost in human resources needed to configure the features properly which may include training and/or implementation assistance. Once implemented, the system should require only standard maintenance (version patches/updates) and periodic validation/testing to ensure that it continues to function as intended.

NOTE: In most cases, IIS utilizing an external hosting service (Amazon Web Services - AWS or a vendor-hosted environment) have already been configured to encrypt both data at rest (AES-256) and in transit (TLS 1.2). For self-hosted environments, it is up to the IIS to configure all their own encryption settings.

Encryption standards do not often change, but programs should ensure that they are always using the most current NIST-approved standards. Any platform leveraged by an IIS should have been tested in a calibration lab and should have received FIPS 140 standard certification (FIPS compliant) and NIST approval. Commercial products like Oracle and SQL Server would have been tested and certified prior to release, which covers most IIS implementations.

For server and database encryption, **Advanced Encryption Standard (AES)** is the current standard approved by NIST.[36] AES 256-bit is the gold standard, but IIS would also receive appropriate protection using AES 198-bit. AES greater than 256-bit (e.g., 512-bit) is unnecessary and may result in a noticeable impact on system performance. Ultimately, a longer key (bigger number) provides a stronger algorithm and more robust encryption; however, for IIS, it is important to establish an appropriate level of protection without negatively impacting the user experience.

The level of encryption necessary should be based on the amount of data, type of data, number of end users, and where the system/data is physically located. An IIS may opt to encrypt the entire IIS database or a selection of data elements that most need to be protected (e.g., patient name, DOB, mother's maiden, SSN). For a database operating in a virtual cloud environment (e.g., AWS) and using shared space, the IIS should encrypt the entire database and logs.

[36] Technical guidance on AES: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Performance parameters are a consideration with encryption/decryption. Adequate resources should be in place to compute the loads generated by a large number of users and large amount of data. This can be done with capacity planning of the environment and ongoing performance monitoring from the end-user perspective. This may also require a database administrator (DBA) to assess logs and identify benchmarks (e.g., the time it takes a transaction end to end). The DBA would evaluate performance both with and without encryption, then determine how to minimize issues – scale the database, limit size of data in tables, assess how the master patient index comes into play.

For data elements where use of hashing is desired, a system should use a **Secure Hash Algorithm** (SHA).[37] There are currently two families of NIST-approved hash algorithms – SHA2 or SHA3. SHA2 is the most common, and either algorithm would be appropriate for use by an IIS. Applying a one-way hash to fields like password ensures that it is always stored as an encrypted string and can never be displayed in a human readable format.

Note: It is possible for the IIS to have multiple levels of encryption in place at the same time. For example, the server is encrypted (Level 1), the IIS database is encrypted (Level 2), and fields like passwords or SSN are encrypted (Level 3). Server-level encryption protects the data if someone were to walk off with the physical server. Database-level encryption protects the data from a hacker or other attack trying to access the data without valid user credentials. Field-level encryption protects sensitive data even from users with valid IIS user or administrative accounts.

For data in transit, the vast majority of transactions carrying data between an external system and an IIS are encrypted for transmission using HTTPS (also called HTTP over TLS or HTTP Secure). **HTTPS** encryption uses the very common and widely implemented Hypertext Transfer Protocol (HTTP). By adding Transport Layer Security (TLS)[38] onto HTTP, it creates a secure channel over an otherwise insecure network.

This technology has been used by IIS for many years for securing both user interface access and electronic data exchange and is the same protocol used by the internet at large for encrypting financial transactions such as online shopping and banking. Once the client (submitting provider/EHR) and server (IIS) are connected (known as the TLS handshake), all transactions between the two connections are encrypted. This can be visualized as a pipe between two systems that is opaque and ensures no one else can read the data inside of it (demographic and vaccination information and authentication credentials).

One challenge of secure data transmission is ensuring that all partners are using the most current version of TLS (currently TLS 1.2). This is ultimately determined by the internet browser used by the provider for interoperability transactions and what version of TLS the browser supports. IIS should push for use of the most current version and not allow for downward negotiation, as this scenario creates security vulnerabilities. Ultimately IIS must find the appropriate balance between interoperability and security.

Note: HTTPS is used for the encryption of routine data transactions that occur between external systems and the IIS throughout the day. Occasionally, a provider may need to submit larger batch data or other ad hoc data transmissions. In these situations, other secure transport methods may be more appropriate, such as Secure File Transfer Protocol (SFTP) or secure email transactions.

Historically, the primary focus for IIS has been on the encryption of data in transit, but recent discussions have turned towards the encryption of data at rest as cyber security incidents become increasingly commonplace. Encryption is especially important for externally hosted environments, and critical if the IIS is operating on a shared server. There is, however, some difference of opinion among the interviewed experts about the ultimate value of encryption of data at rest. Database encryption does not protect against attacks from internal sources (e.g., system/database access using a legitimate user account), which is where most security incidents originate. Encrypting data at rest is of little value if the applications used to access the data are compromised since the application will decrypt the data for a seemingly authorized user. For example, the money in the bank's vault is secure until a bank robber forces an employee to enter the combination and open the door. Encryption can certainly be a useful tool but should always be used in conjunction with other security measures in a layered approach.

[37] Technical guidance on SHA: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html

[38] Technical guidance on TLS: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

In addition to the encryption of the IIS database and data in transit, IIS administrators should discuss the value and IT policies/procedures around the encryption of transportable devices that can be lost or stolen such as desktops, laptops, and portable storage drives where IIS data and reports may be saved locally. Commercial tools such as BitLocker or FileVault may be used to perform this function. At minimum, all workstations should be configured to lock automatically following a period of inactivity (e.g., five minutes) to further protect against unauthorized, passive access.

Note: Encryption is not an activity required by HIPAA, but it is a factor in the Breach Notification requirements.

Conversation Starters:

- ➔ Does the IIS reside on its own server? Is the server hosted in-house or with an external third party?
- ➔ Does the IIS encrypt data at rest? If so, what is being encrypted (server, database, or specific fields)? What version of encryption is being applied? If no encryption is being applied, is the IIS willing to accept related risks identified during the Risk Assessment?
- ➔ Does the IIS encrypt data in transit? If so, what protocols/versions does the IIS support?
- ➔ What ePHI does the IIS store? Is there other "high value" data produced by or stored in the IIS? Would these high-value data elements benefit from additional security (e.g., hashing)?
- ➔ Do the existing levels of protection seem appropriate, or do they need to be reassessed? If not already protected, would ePHI or high-value data benefit from encryption?
- ➔ Does the organization have existing policies around the encryption of workstations, laptops, and/or portable storage devices?

User/Account Management

Unfortunately, the primary threat to data at rest originates with either an authorized user or through a valid user account. Many of the elements that govern user management seem obvious (e.g., username, password, role-based permissions); however, this is an area that can be easily overlooked or not well maintained. While multifactor authentication and smart card technologies are trending as a standard of practice for military, government entities, and high-tech corporations, these methods would be difficult to implement and manage from an IIS user perspective. Tools for implementing multifactor authentication can be very expensive, especially if dongles and/or subscriptions are required. Furthermore, this level of security may be considered inappropriate for IIS because the data contained in an IIS is designed by purpose to be accessible to providers, school/childcare personnel, and even patients themselves through newly evolving patient portals. There are, however, several best practices around user management that IIS should review and use to improve policies and/or IIS feature functionality as needed.

Single User – Single Account:

Every user of the IIS must have their own unique account login credentials. These unique user credentials may also by assigned at the EHR level where users are querying and/or submitting data to the IIS directly through the EHR interface. This practice also extends to sites participating in electronic data exchange. Each site must have unique login credentials to properly authenticate with the IIS. The unique identifiers assigned to each account will then be used to track and identify all transactions that originate with the user/sending site for the purposes of audit logging and incident investigation.

IIS policies and user agreements should explicitly state that sharing account information is strictly prohibited. If an account has been compromised due to sharing, the account should be administratively inactivated from further use.

NOTE: IIS administrators should be mindful of the process for new users requesting access to the IIS. If the process is overly difficult, complex, or time consuming, users may be opting to share credentials or inherit existing credentials without the knowledge of the IIS.

Defining User Roles:

IIS products should include appropriate support for defining/assigning roles based on user need. Users should be allowed to access only the material and system features appropriate to their respective job function and duties. User access should be updated if/when these roles change. Some typical examples include:

- Read only access – user can look up and print a patient vaccination record (receptionist)
- Add/edit access – the user can create new patients, update existing patient demographics, record new vaccination events, or update existing events previously reported (nurse, registrar/recorder)
- Inventory manager – has ability to reconcile a facility's inventory, place a vaccine order, and generate appropriate inventory reports and patient lists (inventory manager)
- Organizational administrator – an administrative account for a user that oversees multiple facilities within a larger umbrella organization, allows them to toggle between multiple facilities, run reports, and possibly oversee the creation of new user accounts for those facilities (office manager)
- Data exchange – has the ability to submit electronic messages or query records through the HL7 interface but may be unable to interact directly with other IIS features (electronic system)

Unique User IDs:

User IDs/Usernames may be assigned by the IIS Program or Help Desk staff, defined by the user, or auto generated by the IIS. User IDs should be unique and not duplicated within the IIS. User IDs should avoid using naming routines (e.g., User1, User2, User3) where the naming can be easily confused. Some IIS may also require a minimum number of characters when defining a user ID.

Password Management:

Passwords should follow industry standard best practices and comply with state/jurisdictional IT policies. Interviewed experts recommended that IIS include support for standard password management strategies, such as establishing requirements for minimum character length, a combination of upper and lower case letters, use of special characters and/or numbers, and restrictions on recycling a previously used password.

Some IIS have these requirements hard coded, while others allow for administrative configuration. IIS administrators should review the current system settings and ensure that they are in line with current recommendations that support security best practices.

In the past, many IIS issued a generic password for all newly established accounts, training accounts, and/or password reset requests (e.g., Welcome1, Password, repeated username). Typically, a user would then reset the password upon first login. The use of generic passwords is not recommended since these passwords can be easily guessed and may or may not get reset by the user. Better practices include using an auto password generator and configuring the IIS to force a password change upon first login. If possible, the IIS could also be coded to prohibit the use of generic passwords.

Note: Passwords should never be emailed in conjunction with a username. Passwords should be provided verbally or through a separate email or text message. The IIS should then force a password change upon first login using the temporary password.

Authentication for IIS Data Exchange:

For electronic data exchange, each site must have unique login credentials to properly authenticate with the IIS. In most cases, this can be accomplished simply using a site-specific username and password. Some IIS may also include a facility code as part of the authentication procedure. Other mechanisms for authentication, such as Public Key Infrastructure (PKI),[39] that involve distribution and management of client-side certificates (or public-private key pairings), have proven challenging for some IIS and have not been widely implemented in the IIS community.

More information on user authentication, password management and common threats can be found at:

- Digital Identity Guidelines DRAFT (NIST 800-63-3)[40] *New*
- Electronic Authentication Guideline (NIST 800-63-2)[41] *Retiring*
- Guide to Enterprise Password Management (Draft) (NIST 800-118)[42] *Historical*

[39] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

System Controls:

Many IIS are coded or configured to support several other best practice behaviors through automated system controls.

- **Automatic Timeout** – These settings will automatically log a user out of the system after a specified period of inactivity (e.g., 10 minutes). This time period may be hard-coded or established as an administrative configuration.
- **Single Instance** (One User, One Instance) – This feature prohibits access by a single account (username/password) on multiple workstations at the same time or multiple instances on a single workstation. If someone attempts to log in to a new workstation (or new tab) while the other session is still active, the previous session will be automatically terminated.
- **Lockouts** – If a user attempts to login with an incorrect username/password combination after a specified number of attempts (e.g., three attempts), the system will automatically lock the user's account to further access. The number of attempts may be hard-coded or established as an administrative configuration.
  - Best Practice: IIS should not give the user any feedback about whether it is the username or password that is incorrect or whether a specific threshold of allowable attempts has been exceeded. User should continue to receive a generic message for each failed attempt – e.g., "The username or password is incorrect."
  - Good Practice: IIS can be configured with a specified time period that must pass before the user can attempt to login again.
  - Better Practice: Once account has been locked, require the user to answer a series of security questions to unlock the account.
  - Better Practice: Have the user contact the IIS Program/Help Desk directly to have the account administratively verified and then reactivated. Policies and procedures should be established for managing the verification process to ensure that the user is who they assert to be (e.g., review the details on the user account, have IIS staff return the user's call to the clinic number on file to complete the transaction, or have the user respond verbally to a series of security questions).
- **Forgot Username/Forgot Password** – IIS can be configured with forgot username/forgot password features that leverage either security questions or the email address/cell phone number on record for the user. Third-party tools like Captcha or other "I am not a robot" tools could also be implemented to verify that the user is human (e.g., "enter the code you see in the box").
- **Expired Passwords** – These settings will automatically require users to reset their password after a specified time period has elapsed (e.g., every three months) and can be applied to both active and inactive user accounts. This elapsed time may be hard-coded or established as an administrative configuration. This feature may also be configured to establish restrictions on recycling a previously used password. *Note: Ideally this protocol should apply to all accounts used to access the IIS; however, with accounts used solely for electronic data exchange (e.g., HL7 interfaces or HIE connections) this may not be feasible and may even be cost prohibitive. IIS administrators should weigh the pros/cons of implementing this practice for active exchange connections.*

[40] https://pages.nist.gov/800-63-3/sp800-63-3.html

[41] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[42] http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Account Management:

While account management can be time and labor intensive, IIS should have appropriate policies, procedures, and tools in place to support this process. At minimum, the IIS should be able to produce an administrative user report that lists accounts that have not been accessed within a specified time period (e.g., 30, 60, 90 days). IIS staff should then review this report on a regular basis (typically monthly) and deactivate inactive accounts. If users attempt access after deactivation, they should be prompted to contact the IIS program or help desk staff to have the account verified, reviewed, and reactivated.

Possibly more difficult to manage are changes in user roles or employment status. If possible, the IIS should include an administrative user report that lists all users with a specified role and/or role by facility. A process should be in place to periodically (e.g., quarterly) review users and roles with the respective facilities to ensure that user access permissions continue to be appropriate and to account for employee turnover.

Note: IIS program and technical/vendor support staff accounts should be reviewed no less frequently than monthly and be deactivated immediately if employment status changes. See also Facility, Workforce and Contracted Security Considerations.

Occasionally, a site/facility may also need to be inactivated due to a variety of issues like closure, mergers, or a change in business model. In these scenarios, the IIS will need a process in place to deactivate all associated user and data exchange accounts.

Audit Logs:

IIS should implement appropriate administrative user reports and logging to identify other elements of user activity. The IIS should also set up protocols for reviewing these reports on a routine basis to look for suspicious behavior and pattern anomalies. Some examples may include:

- **User Access** – to track user activity in the IIS. Report should include User ID, IP address, login date/time, logoff date/time
- **Failed Login Attempts** – to identify possible phishing activity. Report should include IP address, date/time of attempt, and User ID attempted.
- **Patient Record Activity** – to track what the user did while logged into the system. Tracking should be at the patient level and may include the User ID, what they looked at (demographics, histories, reports where the patient was listed), any changes or modifications the user made to the record (additions, edits, deletions), and date/time of event.

Administrators:

Administrative-level users include all "super" users such as database administrators (jurisdiction and vendor), IT management and contractors, IIS administrators, help desk staff, and even provider organization-level administrators. These users typically have a much higher level of access to hardware, features, configurations, and data. Policies and procedures should be created, reviewed, and practiced to ensure that access levels/abilities are necessary and appropriate to the user's role and that access and accounts are deactivated if roles or employment status change.

Unfortunately, these users/accounts are also positioned to do the most harm where ill intent can be paired with knowledge, skill, and access. Administrators can even be targeted from presentations posted online or staff directories where name, job title, and contact information provide clues that can be socially engineered and exploited by hackers to gain access through administrative level accounts. Multifactor authentication (smart card or authenticator tokens) may be more appropriate to implement for this level of user for those IIS interested in moving in that direction.

User Agreements/Site Level Agreements:[43]

Finally, user agreements should be used to communicate the terms of accessing and reporting to the IIS. This applies to both individual user accounts and data exchange accounts. Login credentials should not be released until a signed user agreement is on file. Historically this was managed solely as a paper-based process; however, this is increasingly being incorporated into the IIS login process or other automated routines. For paper-based administration, the user agreement language should be reviewed periodically and updated as needed. When this language is updated, a process should be in place for collecting new user agreements from existing users. For integrated user agreements, the process can be automated to occur as desired (e.g., each login, with each password change, whenever an account is administratively reset, or as part of an annual routine).

Site-level agreements are particularly important for provider organization-level administrators who may have the ability to create accounts for users within their organizations. These agreements outline the terms and expectations of these organization-level super users, including the requirements for user agreements from each user, the process for generating usernames and first passwords, the obligations to update/terminate access with changes in employment status, and periodic security training. A process should also be in place to periodically review and update these site level agreements.

Conversation Starters:

- ➔ What policies or procedures does the IIS program have in place to ensure that each user has their own individual login credentials? What happens if it is determined that a user account is being shared among multiple users?
- ➔ What features does the IIS have in place to restrict user access based on job function and duties? What processes are in place to review role assignments in the IIS to ensure that they remain current and appropriate to the user? How is this process managed for administrative-level users?
- ➔ What are the current password requirements configured in the IIS? Do they follow industry best practices for strong passwords? Do passwords expire? If so, how often, and can a previously used password be recycled?
- ➔ What happens to a user account after multiple failed login attempts? How many attempts are allowed? Does the IIS have a "forgot username/ forgot password" feature? If so, what tools are used to verify the user and reissue credentials?
- ➔ Does the IIS support automatic timeout following a period of inactivity? Does the IIS allow a user to be logged on in more than one session simultaneously?
- ➔ What policies and procedures does the IIS program have in place for reviewing inactive user accounts? Is there a feature to disable account access? What is the process for reactivating a disabled user account?
- ➔ What audit logs does the IIS have in place for monitoring user access, access attempts, and user activity during an active session?
- ➔ Is there a routine process for reviewing and updating language in User and Site Level Agreements? Is there a process for having users and sites renew their agreements on a routine basis? Does the IIS offer security training or educational materials in conjunction with granting or renewing user access?

[43] Additional information can be found in the AIRA Confidentiality and Privacy guide http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf

Electronic Communications

Some IIS can generate text or email messages to patients for notifications like reminder/recall. From a security standpoint, this practice is neither recommended nor discouraged; the value of this feature is ultimately driven by the business needs of the jurisdiction and its users. It does, however, introduce additional security risks that can be easily mitigated through the implementation of some best practice recommendations.

- Log all notification events (user, data/time, patient, notification type)
- If an email or text message generated by the IIS comes back as undeliverable, inactivate the failed address component in the IIS from being used for further electronic communications (note: this action should take place as soon as possible after receipt of the failure notification)
- Ensure that the message is fairly generic and does not contain ePHI[44] (e.g., "Your child may be due for a vaccination. Please contact your provider to schedule an appointment.")

Some IIS may also support the ability to schedule and then email reports that contain patient data. Due to increased concerns about the security of these messages, this practice should be reevaluated. In some systems, the ability to email the actual report has been disabled in favor of a hyperlink or generic notification message that leads the user back to the IIS or a secure file post (SFTP) to view/retrieve the finished report (e.g., "Your requested report is now ready. Please log in to the secure portal to retrieve your report."). Use of secure email is another option that may be considered. It then becomes the user's responsibility to manage and care for the report and its contents in accordance with standard privacy protocols. It is also recommended that the IIS audit logs capture all events in which an individual patient appears on a report generated through the IIS (user, date/time, report where patient appeared).[45]

NOTE: While staff-generated email is not directly governed by IIS security policies and practices, staff and users should always be mindful of best practice guidelines for security, privacy, and confidentiality by ensuring that PHI is not included in plain text and ensuring that any attachments containing patient lists or information are password protected.[46]

Conversation Starters:

- ➔ What electronic communications does the IIS generate? Are the messages generalized or patient-specific?
- ➔ Does the program have a process (manual and/or automated) in place to identify and deactivate bad contact information?
- ➔ Does the IIS send reports that contain patient detail by email?
- ➔ Does the IIS log all events (e.g., electronic communications, reports) in which a patient is specifically identified?

[44] For IIS that are subject to HIPAA, content of emails is governed by the HIPAA Privacy Rule. The Privacy Rule also governs requirements about tracking and retaining data release records. http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf

[45] Idem.

[46] Idem.

HL7 QBP Security Considerations

HL7 QBP (Query by Parameter) requests present some potential security risks for IIS. While interaction with the IIS via HL7 requires a valid user/partner account, and messages in transit are protected using standard encryption protocols, the QBP query/response (RSP) may be particularly vulnerable to attacks initiated by hackers. With VXU (Unsolicited Vaccination Record Update) messages, the worst a hacker could do is flood the system with a series of bad records that could ultimately be backed out of the IIS once discovered. With QBP requests, however, a hacker could automate a process to query every patient record in the IIS database to supply the hacker with valuable ePHI.

There are several strategies that IIS can employ to prevent a possible attack using HL7 Query:

- IIS should return only what is minimally necessary. Ideally, the IIS should simply mirror the information sent by the querying system. The IIS should never send back information like SSN, mother's maiden name, or an alternative/potential address located in the IIS – these fields are better left blank.
- IIS should return only the data elements required to fulfill the business requirements of the query exchange. The IIS should not include information that is not essential for the integration (e.g., SSN, mother's maiden name, or an alternative/potential address) – these fields are better left blank.
- The IIS should not disclose or confirm what fields were used to create the match. Information like SSN or mother's maiden name may be submitted with the QBP and may be used by the IIS as match criteria, but whether these fields match or not should not be confirmed or returned in the RSP message.
- IIS should not respond with a potential match based solely on the patient ID assigned by the IIS. Many IIS have patient IDs that are generated as serial numbers. A hacker could start at patient ID Number 1 and work their way up pulling out each patient record. The IIS can use the patient ID for the initial lookup but should confirm a match only when other information in the query message, such as name, date of birth, and/or address, support the match.
- IIS should establish hourly or daily caps for queries at the site level, especially for providers that have low security level credentials (e.g., small clinics assigned a simple username/password might be limited to 100 queries per day). These settings should be administratively configurable by the IIS based on the size of the provider, type of practice, and volume of typical submissions.

Intrusion Detection and Alerting and IIS Audit Logging can also be leveraged to detect query-based attacks and identify the extent of the attack should a breach of this nature occur.

Conversation Starters:

- ➔ Does the IIS offer HL7 QBP/RSP support?
- ➔ What data elements are providers required to submit in the QBP?
- ➔ What data does the IIS return in the RSP? How are high-risk data elements handled in the RSP – are they mirrored, stripped, or updated? Is the IIS supplying any information in the RSP that the submitter didn't already supply in the QBP?
- ➔ What match criteria is the IIS using? Does the submitter receive any feedback on what did/did not match?
- ➔ Are there changes that need to be made to IIS features/functionality or policies/procedures for the support of HL7 QBP/RSP?

Section 4.2: Detection

Even with tools and processes in place to prevent security events, attacks (or attempts) can and will occur. The IIS should be equipped to identify suspicious activity or data as quickly as possible. There are several mechanisms that can be used to detect a breach or attack. The approaches vary from sophisticated intrusion detection software to simple manual review of logs and individual patient records. Public facing sites, like IIS, may be more susceptible to a breach or attack because individuals can log in and gain access to back-end information. Malicious software or intrusive activity can also be introduced at various points in IIS workflows or processes with the ability to collect, hijack, or destroy data. As such, the IIS should be equipped with tools to identify abnormal activity in real time as it is occurring or shortly thereafter through routine administrative reviews.

Intrusion Detection and Alerting

Intrusion detection tools act as sensors to log and monitor all system traffic and issue alerts when there is abnormal activity. These tools simply monitor IIS or network activity through a passive, automated process. The tool is configured to identify any deviations and anomalies in behavior patterns (failed responses, performance oddities). The IIS Program (or IT staff) defines what "normal" system behavior is, identifies what anomalies they are interested in looking for (e.g., larger than normal data movement during a specified time period), and then configures the tool to alert accordingly.

There are several products on the market that can perform this service (Snort, McAfee, Juniper, Palo Alto, Trustwave, etc.). These tools can be used alone (good practice) or in conjunction with intrusion prevention tools (better practice). Tools like AWStats may be helpful for IIS staff to establish baseline trends like typical usage, response times, browser stats, number of robots hitting the website, etc. The challenge for IIS administrators is how to sift through all the data to identify meaningful trends and fine tune the thresholds for alert notifications. IIS/IT administrators may want to investigate Security Information and Event Management (SIEM) tools such as Splunk, Logwatch, or LogCheck that can be used to help identify meaningful trends by analyzing audit logs in near-real or real time and generating alerts.

Where intrusion *detection* is a tool for passive monitoring, intrusion prevention provides an immediate counter response to a suspected intrusion alert. This practice may be referred to as "locking and blocking." Intrusion prevention tools can be configured to lock down a specific IP address from further action or disable a user or access port until the issue can be further investigated and resolved. See also Attack Mitigation.

Many solutions hosted through AWS or IIS product vendors already provide intrusion detection and prevention services as part of the standard service solution. These services may be further described in the BAA or SLA.

For more advanced technical guidance on intrusion detection refer to the Guide to Intrusion Detection and Prevention Systems (IDPS) DRAFT (NIST 800-94 r1).[47]

IIS Audit Logging

Most IIS have established extensive audit logging processes. These audit logs provide information on user access, failed login attempts, and activity related to patient and vaccination records.

- **User Access Logs:** IP address, user ID, date/time logged in, date/time logged off
- **Failed Login Attempts:** IP address, date/time, and user ID attempted
- **Patient Record Activity:** patient and vaccination level views, additions, edits/modifications, deletions, inclusion on reports, user ID, data/time of event

Some of this logging detail is readily available through administrative reports built into the user interface, while others may require the assistance of a database administrator to run a specialized query. The audit logs and reports can be used preventatively and forensically. For instance, failed login attempts from a specific IP address can be analyzed for the following:

- How many total attempts to log in were made from that specific IP address?
- What usernames was the user attempting?

[47] http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

- When did the attempts occur (same day, late at night, every day at noon)?
- Did the IP address ever succeed with a successful login (user access log)? If so, what username was used?
- What patient/vaccination records did the user touch during the suspicious, or even previous, sessions (patient record logs)?
- Was the activity appropriate based on the roles/permissions/facility of the logged in user?
- Does the account need to be inactivated pending further investigation?

IIS administrators should have a standing routine for reviewing and analyzing these results. This process should occur as frequently as resources allow to identify breaches and breach attempts as early as possible and initiate an appropriate response to the incident. SIEM tools (e.g., Splunk, Logwatch, LogCheck) may be helpful for analyzing audit logs and identifying trends that deviate from the norm.

Manual Review of Individual Records

Occasionally, a user may happen upon a record that looks suspicious – e.g., the record appears to have been modified inappropriately, fields have been populated with nonsensical values, or the record is no longer available when queried. Users should be trained to notify the IIS staff immediately in these situations so the issue can be further investigated. The issue could be as simple as a mismerged record during the deduplication process or a record that was accidentally deleted. It could also signal something more significant like malware or a rogue user. These reports should be handled on a case-by-case basis with more expansive investigation if needed using other IIS tools or DBA support.

Conversation Starters:

- ➔ Does the organization leverage an intrusion detection and alerting tool? Does the monitoring include IIS activity or just network activity? What tool(s) is/are being used and what activity is being monitored? Can additional activities be added to those currently monitored?
- ➔ Who receives the intrusion alerts? What is the protocol for performing further investigation and notifying other key players? Is instruction detection paired with intrusion prevention?
- ➔ What audit logs does the IIS have in place for monitoring user access, access attempts, and user activity during an active session? Is there a process for reviewing these on a routine basis?
- ➔ Is there a procedure that users should follow if they identify records that don't seem quite right?
- ➔ What policies and procedures does the IIS program have in place for investigating and addressing suspicious activity?

Section 4.3: Response

If a security incident does occur, the IIS should be prepared to respond accordingly depending on the nature and extent of the event. For instance, a small-scale response to suspicious activity from a specific IP address can be handled manually or through intrusion prevention tools by blocking access from that IP address; whereas, a large-scale event like a natural disaster will require the activation of a formal Response Plan. If patient data has been knowingly or potentially compromised, the IIS may also have a legal or ethical obligation to notify patients of the nature and extent of the security event. The following sections describe some primary considerations around Response Planning, Contingency Operations, Attack Mitigation and Breach Notification.

Response Planning

An important element of IIS security planning is preparing for a possible incident regardless of whether the incident results from a physical event, such as fire, vandalism, system failure, or natural disaster, or a cyber event, such as those initiated from an external or internal source. Response Plans may include a variety of components (e.g., Contingency Planning, Emergency Mode Operations, Disaster Recovery, Data Recovery/ Restoration) and should address the following:

- Identification of all key players and assignment of appropriate roles and responsibilities*
- A process for determining what elements of the network or IIS have been affected, identifying the source, implementing appropriate mitigation strategies, and assessing the extent of any damage to hardware, software, or data (see also Detection)
- Activation protocol for contingency operation alternatives
- Notification and documentation requirements
- Recovery and restoration of the IIS (see Recovery)

**NOTE: As IT operations increasingly move towards a centralized or contracted IT approach, IIS program administrators may encounter additional challenges in relation to response planning. Identification of specific contacts/key players may be difficult. Reporting an issue or response time for resolution may be impaired by new processes and competing priorities. Familiarity with the IIS specifically may be reduced by varying levels. Documentation, especially for response planning, may be outdated or too generalized. While centralized or contracted IT operations make sense from a budgeting and efficiencies perspective, it potentially creates additional concerns that should be accounted for in planning for and responding to an IIS security event.*

Response Plans should be reviewed, updated and tested on an annual basis. IIS administrators are encouraged to contact their emergency preparedness counterparts for sample text or for assistance with testing of plans and various response scenarios (see also Contingency Planning).

Conversation Starters:

- ➔ Does the IIS have a formal written Response Plan? Is the plan customized to the IIS? What type of events does the plan cover? Does the plan include components for (1) detection/ investigation, (2) contingency/emergency operations and/or (3) recovery/restoration?
- ➔ Does the Response Plan include a full list of key contacts, including roles, responsibilities, and contact information?
- ➔ How often is the plan and contact information reviewed and updated?

Contingency Planning

An important part of response planning includes maintaining and/or restoring access to the IIS data and feature functionality as quickly as possible after an event has occurred. Contingency planning establishes the protocols and infrastructure for continued IIS operations in situations where the primary instance of the IIS has been compromised or general access to the IIS cannot be readily restored.

A basic Contingency Plan can be created or revised using the following guidelines and by leveraging elements from both the Risk Assessment and Response Planning activities:

1. Identify all key players. Include the designation of the System Owner/Operator who is ultimately responsible for all financial and operational decisions related to the IIS. See Response Planning.
2. Look at every workflow or process associated with the IIS and determine where possible failures could occur at each step. Document all systems, applications, and data. This activity can leverage the work performed during the Risk Assessment.
3. Identify a three-layered response approach to each item. If one part fails, what should happen next? If that part fails, then what? Focus initial efforts on high-risk/high-priority failure points, followed by medium- and then low-risk items.
4. Include roles and responsibilities for each response activity including the methods of contact for each key player in the various response scenarios.

The NIST resource titled "Contingency Planning Guide for Federal Information Systems (NIST 800-34 r1)"[48] may also include helpful guidance to IIS programs in the process of drafting or revising a Contingency Plan.

Contingency Plans should be reviewed and tested on an annual basis, with updates to the documentation as needed. Some tests may be accomplished using a simple checklist or tabletop simulation exercise, whereas others may require an actual test of a specific system function (e.g., database server goes down, failover goes live) or full "worst case scenario" exercise (e.g., perform a complete rebuild and restore).

Full recovery testing is very important but can also be very expensive. Some agencies may not have the budget or staffing resources to administer a full-scale testing effort. As with general response planning, IIS administrators may want to consult their emergency preparedness counterparts for assistance with testing of plans and various response scenarios. The following narratives describe a couple of scenarios where contingency operations may be necessary.

Conversation Starters:

- ➔ Does the IIS have a formal written Contingency Plan? Is the plan customized to the IIS?
- ➔ Does the plan include a full list of key contacts including roles, responsibilities, and contact information?
- ➔ Does the plan include multiple layers of contingency in case the previous layer fails?
- ➔ How often is the plan and contact information reviewed and updated? How often is the plan tested?

Scenario 1: IIS is taken offline

An IIS can be taken offline for a variety of reasons: catastrophic event, power failure, hardware theft, cyber attack, system malfunction, or even routine maintenance and upgrades. Regardless of the reason, the first priority in contingency planning is to provide continued access to IIS features and data. This can be accomplished through the establishment of a failover environment or "hot site." If the primary instance goes off line for any reason, the IIS should have a failover in place that goes live automatically or a "hot site" that can easily be brought online. This transition should be as seamless as possible to the end user.

The failover system should provide a full mirror image of the IIS including adherence to all the same security requirements and protocols as the primary IIS: jurisdictional IT security policies and procedures, facility and system access controls, hardware and network safeguards, operating platform, configurations, IIS features/capabilities, and the contents of the primary IIS database. Nothing should change except the actual location of the hosting server.

[48] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

In some cases, the IIS administrator may be able to participate in a site visit to the failover site; however, in other cases, the failover may be hosted in a Cloud environment or at a secret location. If the system is hosted in a virtual environment or offsite location, the IIS administrator should be familiar with whether the failover is being hosted on an individual server or one that is shared with another system. If the system is on a shared server, this may require additional security measures like full server-level and system-level encryption. In either scenario, the IIS administrator should be familiar with what security assurances the hosting environment provides and how those align with jurisdictional IT security policies. The IIS administrator should also be familiar with any SLA language around guaranteed system "up time" and response times.

Regardless of where or how the failover system is housed/hosted, the IIS administrator should have a documented chain of contact for all parties with roles and responsibilities in facilitating the changeover. This list should be routinely reviewed and updated. IIS administrators should also consider the following lessons learned offered by the interviewed security experts (unfortunately, many of these better/best practices arise from previous failures):

- Failover system should have adequate geographic separation from the primary IIS instance (e.g., located at least five hours away). Local and mid-range locations have potential to be impacted by the same event, especially those resulting from a natural disaster (flood, earthquake, hurricane, tornado, etc.).
- Failover facility should be required to have a backup generator to prevent a double down scenario. In a reported event, the primary instance went down and switched over to the failover site; however, the failover site was affected by a local power outage leaving both the main system and the failover system inaccessible. It is also important to know how long the generator can function.
- The failover system should be updated daily and no less than weekly. Some systems may even opt to update in real-time. The frequency for how often the database is replicated depends on the user's tolerance for the absence of recently entered data that is accounted for in the replication delay.
- Automate the switchover process – when one system goes down, the other should come online immediately. The transition from the main system to the failover system should be virtually seamless to the end user. In a reported scenario of an actual event with a manual transition, it was difficult to find a resource/contact that could perform the switch at the time of the actual event.
- Test the failover system no less than quarterly. If resources are available, test monthly to make sure there are no issues with the hardware or software.

For some jurisdictions, real-time replication to a failover environment may be cost prohibitive. In these cases, the IIS should replicate daily or weekly or be prepared to apply the most recent data backup (see Data/Database Backup Procedures and Restoration). The IIS should have a documented process for how the data replication or backup restore procedure will be managed. Alternatively, some jurisdictions may specifically choose not to perform real-time replication. As cyber-attack strategies become more sophisticated, threats like ransomware can follow the data and take down both systems simultaneously. In this case, delaying the update of the failover or hot site database by a specified time period may be preferable.

Further, some IIS programs may not have a failover system or hot site location established at all. While this practice is not recommended, programs in this situation should have detailed procedures documented for building a new environment and bringing it online as quickly as possible. The IIS should know how long it will take to complete this process from start to finish and should test the procedure on an annual basis, at a minimum. See also Data/Database Backup Procedures and Restoration.

Conversation Starters:

- → Does the IIS have a failover environment or hot site? How far away is the failover environment from the primary instance of the IIS? Does the failover/hot site have a power generator?
- → How closely does the security infrastructure for the failover mirror that of the primary instance? Is it possible to participate in a site visit or security audit of this location?
- → Is the changeover manual or automatic? If manual, how quickly can the failover be brought on line? How often is the data in the failover environment refreshed? How often is this procedure tested?

Scenario 2: Access to the IIS cannot be readily restored

During a security event, operations may be widely affected (statewide) or impact only users in a single area/region ("the panhandle" or state capital). As IIS are increasingly used for more than patient records (like ordering and inventory management), the main priority is that access to the IIS remains unaffected as much as possible and that, if access cannot be restored, other options exist for data collection. Contingency Plans should include flexibility for the continued collection of vaccination data through any means possible and provide at least three layers of contingency for user access and reporting:

- Priority 1: Maintain/Restore System Access
- Priority 2: Leverage a Standalone Application
- Priority 3: Provide a Paper-Based Option

System Access:

The primary goal is to restore access to the IIS as quickly as possible. This typically involves maintaining a failover or hot site environment, as previously described, so the end user is minimally impacted. If both the main system and failover environment are equally impacted, it becomes a matter of how quickly the systems can be rebuilt and restored from the ground up.

Standalone Application:

While general access to the system may be restored, some users may continue to lack internet or telephone/cellular availability to access the system online. In this scenario, the IIS should be prepared with the flexibility to capture data through a standalone application, especially with long-term compromised access or if trying to vaccinate people in an evacuation shelter environment. Standalone applications can capture patient and vaccination details and be uploaded to the IIS when possible. Emergency Operations Centers (EOC) may also need this type of data for making decisions when managing active response situations.

Standalone applications can be loaded onto laptops and/or portable storage devices for distribution through strike teams. Portable devices should be configured in accordance with state IT policies to ensure that all security features have been appropriately configured. A centralized contact should be designated to manage the distribution and chain of custody for each device. Once data has been collected, all hardware/devices should be returned to the specified contact for uploading of data to the IIS and proper cleansing or disposal of the device itself. See also Hardware Management.

Paper:

When lack of access and other resources (no access to power, not enough laptops or human resources) persists, the IIS should be prepared to capture the data anyway possible, which usually means resorting to paper. Data collected using paper methods should then be entered into the IIS as soon as possible after access has been restored. The longer data entry is delayed, the less likely it is to ever be entered into the IIS. For security purposes, paper records may be subject to slightly different rules than ePHI. Paper records should be managed in accordance with state policies for patient record storage and destruction.

Conversation Starters:

- ➔ What is the IIS program's maximum threshold for downtime (no access or severely restricted access) before alternative data collection methods are implemented? Does this policy apply only to statewide/jurisdiction-wide outages or also localized outages?
- ➔ Does the IIS have a standalone version of the application that can be used remotely? If so, how is this standalone version accessed/distributed? What is the chain of custody for devices used to collect data? What is the process/procedure for getting the data back into the IIS? What is the process/procedure for clearing data from the devices used for collection?
- ➔ What is the policy/procedure for data entry when users have to resort to paper-based data collection?

Attack Mitigation

Another element of response planning is mitigating or halting an event in progress to whatever extent possible. Suspicious activity may be identified through alerts issued by Intrusion Detection tools, through the diligent review of IIS audit logs, or by happening upon a record that looks questionable. Response Plans should include guidance on the policies and procedures for determining what elements of the network or IIS have been affected and identifying the source of the attack/event. At this point, the IIS should implement appropriate mitigation strategies to hinder or stop the attack. This may be accomplished using manual techniques or by relying on automated tools.

Manual response procedures may include measures such as taking the IIS offline to prevent further damage, blocking an IP address from further access to the network or IIS, or the inactivation of a user or administrative account. The downside of manual response efforts is that by the time the breach or incident is detected, the damage may already be done. An automated response may be more likely to minimize data loss or system failure by interfering with an event in progress.

As previously described, Intrusion Detection and Alerting tools are configured to provide constant, passive monitoring of the activity on the network and in the IIS based on defined baseline or threshold levels. When the allowable threshold is exceeded, the IIS or IT administrator is alerted to the abnormal activity. At this point, an Intrusion Prevention tool can also be engaged.

Intrusion prevention tools are designed to act on the alerts raised through intrusion detection instruments by providing an immediate counter response to the suspicious activity. Intrusion prevention tools can be configured to lock down a specific IP address from further activity or disable a user or access port until the issue can be further investigated and resolved. This practice may be referred to as "locking and blocking." Intrusion prevention tools provide an additional layer of reassurance because the attack can be interrupted early and minimize damage to the system or data.

Most contracted hosting services include intrusion detection and prevention as part of the standard hosting package. IIS using a hosting service should review their SLA or BAA to confirm whether these tools are included and what activities are being monitored.

For more advanced technical guidance on intrusion detection and prevention, refer to the Guide to Intrusion Detection and Prevention Systems (IDPS) DRAFT (NIST 800-94 r1).[49]

Conversation Starters:

- ➔ Does the organization leverage an intrusion detection and prevention tool? What tool is being used? What activities is the intrusion prevention tool configured to respond to, and what actions does it take?
- ➔ When an intrusion is prevented, how is the IT and/or IIS Program notified? Who is notified? What are the policies/procedures for investigating and responding to an event notification?
- ➔ If an intrusion is discovered through a report from a user or through the routine review of audit logs, does the IIS have a formal written policy/procedure for how to investigate, report, and respond to a possible incident? What actions can be taken by staff to prevent further damage?

[49] http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

Breach Notification

After an event has been detected and halted, response planning should include guidance on assessing the extent of any damage to hardware, software, or data. This includes identifying any patient records that may have been inappropriately accessed or compromised as a result of the incident. When patient records have been involved, the IIS may have a legal or ethical obligation to notify patients of the nature and extent of the security event.

Per the HIPAA Breach Notification Rule, Covered Entities (CEs) "must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions."[50] Breach notification policies and procedures should address the following components:

- What constitutes a breach
- Methods to determine the extent of the breach
- Protocols for determining whether the breach requires notification
- Process for reporting the breach including who should be notified and how that notification should occur
- Implementing the Risk Assessment and Response Plans to address the cause of the breach and update prevention and response protocols as needed

The HIPAA Breach Notification Rule also makes a key differentiation between secure versus unsecured PHI. The Rule specifically applies to "unsecured protected health information" defined as PHI that "has not been rendered unusable, unreadable, or indecipherable to unauthorized persons using [an approved] technology or methodology." The primary methods of securing PHI are encryption and destruction. These methods are discussed in more detail in the sections on Data Protections/Encryption and Hardware Management.

The HIPAA Breach Notification Rule provides distinct guidance on what constitutes a breach, how to assess whether a breach requires notification, and the process(es) required to report a breach based on the various levels of severity. While not all IIS are governed by HIPAA, all IIS should consider and document their approach to breach identification, notification, and resolution as noted in the checklist above.

For more information visit, the HIPAA Breach Notification Rule website: http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Conversation Starters:

- ➔ Does the IIS have a documented policy/procedure for investigating a possible breach that involves patient records?
- ➔ Does the IIS include tools that can identify patients that have been added, modified, deleted, or viewed during a specific time frame or by a specific user or IP address?
- ➔ Does the IIS Program have a written policy/procedure for notifying patients when there is evidence that their record may have been compromised in some way? Does the policy apply differently if the compromised records were obtained through the user interface, a stolen device, or from paper records?

[50] http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Section 4.4: Recovery

Following a security incident, the IIS should have appropriate policies and procedures in place to restore the IIS using data and database backups to resume normal operations as quickly as possible. The IIS must also be prepared to document the details of the event, review fail points, and reassess the various administrative and technical controls supporting IIS security. The following sections address Data/Database Backup Procedures and post-event activities.

Data/Database Backup Procedures and Restoration

Data and database backups can be used to protect the integrity of ePHI, prevent data loss, and provide a forensic record of all data and database changes. Backup files can be used to revert the data to a specified point in time prior to the security event or to rebuild/restore the database after the threat has been identified and remedied. While some data loss may be inevitable, a good data backup routine will minimize losses and aid in the process of restoring the IIS.

Backing up "data" in the IIS can encompass a variety of elements: patients and vaccinations, transactions, system logs, the entire database including configurations, and even third-party support software/operating system configurations and the IIS code itself. What gets included in backup procedures is ultimately determined by the criticality of the system and data, and the associated risks of data loss. The act of backing up this data can occur at various times depending on what data is being preserved and what tools are being used to perform this function. These frequencies may vary from every few minutes to nightly, weekly, or even monthly. IIS administrators should document these procedures: what systems are being backed up, what data is being included in the backup, how the backup is being performed (tools and process), how often, how long backups are retained, and who is responsible for overseeing this process.

For many IIS, data backup tools are included within the actual database platform (e.g., SQL Server, Oracle). The backup tools can be used to perform both full and differential backups of system data and logs at frequencies established by the system administrator. Differential backups (or redo logs) save just the data modifications occurring in the system. These short-term backups are configured to occur at a high frequency (e.g., every 15 minutes, usually no longer than one hour) and can be used to back into the exact point of failure if needed. Commercial products can also be added to these systems for additional backup feature functionality. For instance, some "smart backup" tools can be configured to automatically perform a backup based on a threshold configuration (e.g., real-time, every two hours, or whenever 250 MB of data have changed).

A full backup represents a snapshot view of the entire database (transactions and data at rest) at the time it is performed. These backups should be performed on a nightly basis as part of a standing automated routine. Managing and scheduling backups are typically part of standard IT protocols. Some programs may also conduct weekly backups to capture all IIS data, logs, transactions, and configurations. Additionally, some programs may go even further by performing server-level backups monthly to capture all server-level settings/configurations and third-party software tools leveraged by the IIS. The extent and frequency for backing up data (and systems) ultimately depends on how much "data loss" a project is willing to assume if there is an incident that requires the system or database to be restored from backed up data.

NOTE: The terms "hot backup" and "cold backup" may come up during discussions on IIS backup practices. A hot backup refers to a system that remains live and online while the database backup is occurring. A cold backup refers to a system that is frozen from use while the backup is performed. IIS administrators should be familiar with the practice used by their jurisdiction, but either practice is acceptable.

Performing Backups:

Data may be backed up to another server located either within the primary hosting facility or at an established offsite location. Data may also be backed up to a virtual hosting environment, like Amazon Web Services (AWS). While backing up to a physical or virtual server is the preferred method, some jurisdictions may simply back up to physical tape or other removable media as either their primary backup method or as an additional preventative measure (e.g., weekly snapshot). While each option has its merits, where data backups are concerned, there is a hierarchy of good, better, and best practices:

Good – Backups are critical, so simply having a backup of any sort is a good practice! (1) Backing up to physical tape or other removable media requires additional administrative considerations such as chain of custody, physical storage location, data protections on the media itself (e.g., encryption), cataloguing schema, and destruction protocols for when the life of the media has been expended. (2) Backing up to a server located within or near the same facility where the primary system is hosted presents the possibility that the backed-up data could be subject to the same physical or network threats as the primary system.

Better – Backing up to a remote location. Whether the system is being backed up to an external server farm or virtual environment, the remote location provides an additional layer of protection from physical or environmental threats that may impact the primary IIS instance. It is important, however, that the external environment is subject to and protected by the same security measures and policies as the primary system. It is also important that backups are transmitted over a secure VPN to the remote environment.

Best – Backing up to a remote location that is offline. New CryptoLocker and other ransomware threats lie in wait to follow the data backup and then ultimately hijack both the primary and backup systems. These tools have already evolved to a point where they can engage even without the user clicking on something to execute the program. Breach monitoring sensors can look for this type of "command and control" activity, and then intrusion prevention tools can shut down the user location (see Intrusion Detection and Alerting for more information).

Retaining Backups:

The length of time that backup records are retained depends on the type of information stored and generally falls under jurisdictional IT policy. For instance, log files and transactions are typically kept for 30-90 days and are then often archived or aggregated using a log aggregator tool such as Trustwave. When a possible breach is suspected, forensic investigations evaluate activity trends over time and look for anomalies in typical use patterns. For other database records, the retention policies for backed-up data may vary by individual state and IT policies. Typically, these backup files are stored for 7-14 days before they are deleted or overwritten. IIS administrators should visit with their IT counterparts to find out what the current policies and practices are to ensure that they meet the needs of the IIS.

As mentioned above, some tables (HIPAA reportable logs, system access logs, HL7 messages) may be archived off to a separate database for longer-term storage purposes or aggregated into a master log using a log aggregator tool. Archiving is a good strategy for storing data that is unlikely to be viewed or changed. Data archiving is included with standard operating platform configurations and generally requires no special tools. *Note: Historically archiving media has been a challenge because the data remains stagnant as the storage technologies evolve (writeable tape > writeable disk > storage drive). Newer cloud-based storage options may provide a more viable, long-term solution for long-term record storage.*

Archiving should occur according to a routine timeline (e.g., every 30, 60, or 90 days), and the length of time these archives are maintained is determined by IT and/or IIS system administrators. When logs are scheduled to be removed from the archive, this process is typically performed by a DBA who deletes the tables/files so they are no longer retrievable. This process should be documented (who is responsible for this activity, what logs or files should be archived, how often should data be archived, how long should archived files be retained), and a log should be maintained to track when the archiving process has been performed (date/time, who performed the archive, what tables/files were included).

NOTE: Any machines or devices where backed-up or archived data reside must be subject to all the same security precautions and measures applied to the primary database. In addition, IIS administrators should discuss hardware management, data destruction protocols and encryption with their IT system administrator, especially where any portable media may be involved (e.g., physical back up tapes).

Testing Backups:

Since data backups are a critical component for maintaining data integrity, investigating breaches, and restoring data following a physical incident or cyber attack, it is important to periodically review the procedure, as well as the actual backup file. Backup files should be opened and inspected to make sure the file (1) contains data and (2) is backing up what it is supposed to be backing up. This data check process should be performed monthly and no less than quarterly. It may

also be a good practice to keep a log of when a backup is performed, what data/files were included, and who/what performed the actual backup procedure. A similar log should also be used to capture the periodic review of these files.

On an annual basis, the IIS should attempt a full data restore from backed up data. This process represents the true test of whether the IIS backup is capturing the correct data and whether the system can be appropriately restored. If this process fails, the data backup or backup process has failed and needs to be immediately reassessed.

Other Backup Considerations:

While this section focused primarily on backing up the IIS database, it is also important to back up the third-party support software and operating system/server configurations, as well as the actual IIS code set. If a system suffers a server-level attack or must be restored from the ground up, the framework that supports the actual IIS application (operating system, supporting software) will need to be restored before the IIS and IIS database can be reestablished. These backups can be accomplished in conjunction with other backup routines. Code backups are typically managed by the IIS vendor or development staff and are stored in a code repository. This process is generally performed using a commercial product such as Atlassian/Confluence Bitbucket. Code backups protect against changes in the code that may introduce undesirable behavior with new version releases.

From a response perspective (e.g., natural disaster, mass vaccination event), code integrity and ability to revert to a previous version are increasingly important. Code that is developed "on the fly" to address a particular incident/event typically does not follow the standard software development lifecycle and may inadvertently introduce bugs or break other critical features due to limited time for proper requirements gathering and adequate regression testing. When there are rapid code and version upgrades, it is important to have a process in place for restoring a prior version as quickly as possible if needed. In these scenarios, some data loss may be inevitable.

For more information on data backup protocols, see also "Contingency Planning Guide for Federal Information Systems (NIST 800-34 r1)."[51]

Conversation Starters:

- ➔ Does the IIS have documented procedures for IIS data, database, and server backups – who oversees this process, what data is backed up, how this process occurs (tools used), how often this process occurs, where backups are stored, how long backups are stored?
- ➔ What security mechanisms are in place for protecting the backed-up data?
- ➔ What is the extent of data loss the IIS Program is willing to accept in the scenario that the IIS system or database must be restored from a backup file?
- ➔ Is there a documented routine for reviewing backup files for content? Is there a testing protocol for ensuring that the system can be restored from the backup files?

Update Documentation, Policies, and Technical Controls

Particularly after a data breach or cyber attack, it is important to document the details of the event and the response efforts. Key players should be convened to review all fail points and the circumstances that contributed to the failure. The various administrative and technical controls should then be readdressed with new or modified tools/strategies implemented as needed to ensure that the vulnerability has been adequately addressed. This may also require updates to policies and procedures or a revision of the previously administered Risk Assessment.

For more information on recovering from a cyber attack, see also "Guide for Cybersecurity Event Recovery (NIST 800-184)."[52]

[51] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[52] http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf

Section 4.5: Administrative Policies and Routines

Administrative policies and routines encompass several administrative elements that expand beyond just the IIS yet have direct relevance to the overall IIS security strategy. IIS administrators should be aware of their local jurisdictional laws and practices and should be prepared to provide input where possible. The following sections will address general practices around data retention and destruction, hardware management, facility and workforce security considerations, and basic security maintenance routines.

Data Retention and Destruction

Patient data (name, date of birth, personal identifiers, address) in the IIS is both the cornerstone of an Immunization Record and the most prized information to those who wish to do harm (e.g., fraud, identify theft, people finding). Furthermore, many IIS operate as birth-to-death registries and contain hundreds of thousands of patient records. This data at rest in the IIS is susceptible to both internal and external security threats.

Patient record retention in the form of electronic records is becoming an increasingly popular topic of discussion. While e-health records differ in nature and purpose from their paper predecessors where retention requirements were clearly defined, guidance on this topic is generally lacking. As cyber attacks and technologies become more sophisticated, this issue becomes increasingly important as IIS weigh risk and responsibility. Legally and ethically, the data "owner" is required to protect this data in accordance with federal, state, and local laws until the point at which it is destroyed. Some questions that the IIS community should be discussing include:

- When is a record determined to be inactive from the global IIS perspective (e.g., death or no patient level activity for 25 years)?
- Should an inactive record be archived? Should that record be completely removed from the database at any point? If so, what are the conditions that should define those actions, and what process should be used?
- What are the risks of maintaining an inactive patient record? Is the IIS willing to assume the ongoing responsibility for the safety and security of that record?

In some cases, state/local level policy may already exist to address some of these questions. IIS administrators are encouraged to discuss these policies with a Records Management Specialist in their jurisdiction. It is likely that state/local policy has already defined, to some extent, what types of data should be archived, how long records/data should be retained, and the process for how/when it is destroyed.

While most IIS do not archive patient and vaccination data in the production database, some IIS do offer feature functionality to identify and archive patient records that have been dormant (no searches/no modifications) for a specified period of time as defined by the IIS program. This process is typically run on a weekly or monthly basis.

When it comes to record removal (deleting a patient record), most IIS perform "soft" deletes, meaning that the record remains in the actual database but becomes locked and no longer viewable to an end user. A true removal ("hard" delete) of the record from the IIS database can be performed only by a DBA through a back-end process. This also requires that all instances of the record and associated data are removed from wherever it may be stored (e.g., tables, files, backups, archives). In these cases, the records may continue exist in memory, and the remnants of the record could still be retrievable by a savvy hacker. Only data purging or hardware destruction techniques can remove the record completely (see Hardware Management).

The following resources include additional information on data retention and destruction:

- Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (NIST 800-122)[53]
- State Medical Record Laws[54]
- AHIMA Retention and Destruction of Health Information[55]
- Medical Record Retention and Media Formats for Medical Records[56]

[53] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[54] https://www.healthit.gov/sites/default/files/appa7-1.pdf

[55] http://library.ahima.org/doc?oid=107114#.WKnmgzvyuUk

[56] https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/SE1022.pdf

Hardware Management

Hardware management typically falls under the purview of the IT department and includes the procurement, configuration/security, chain of custody, and destruction of hardware devices. *NOTE: If the IIS is leveraging an external hosting option, hardware management policies and procedures should be reviewed with the service provider and be clearly stated in the BAA or SLA.* For the purposes of this document, hardware devices include everything from servers for hosting to workstations/laptops. While portable devices like thumb drives and portable hard drives may be procured under the umbrella of office supplies, when used in conjunction with IIS activities these devices should be subject to the same IT policies that govern hardware protections, chain of custody, and destruction.

IT staff are typically responsible for ensuring that hardware is properly configured and maintained as part of standing IT routines. The IT department also generally oversees the configuration and distribution of all workstations and laptops, including the management of network access accounts for employees. All workstations and laptops should be configured to autolock after a period of inactivity and should be encrypted in case they are lost, misplaced, or stolen. If possible, all portable support devices (thumb drives/hard drives) should also be encrypted and/or password protected in accordance with IT policies. User hardware should be scrubbed periodically to ensure that ePHI is not being collected or stored locally. *Note: The IIS should have a standing policy that patient data and/or patient level reports should never be downloaded or stored on personal laptops or personal storage devices.*

All hardware devices should follow a strict chain of custody that is documented by the IT department. This documentation should include serial numbers, hardware description, responsible assignee, date of assignment/starting date of service, date of return/end date of service, and final disposition of the hardware device (destroyed, stolen, sold/donated).

Each piece of hardware has a durable life expectancy and should be replaced after the hardware reaches the end of its useful lifespan (e.g., a server should be replaced every two to four years).[57] When the durable life of a hardware device has been expended or when the device is being reallocated, all data must be removed from the device before it can be disposed of or reissued. When it comes to hardware cleansing and/or destruction, there are three basic levels of data removal: Clear, Purge, and Destroy. The appropriate level of destruction/removal ultimately depends on how important the information is and whether the hardware or data/database is still in active use.

Clear – "Clear" is a simple delete where files or records are removed from view but continue to exist in memory. This is the process that occurs when a user deletes a file from their workstation and empties their recycle/trash bin. Ultimately, data-scavenging tools could be used to bring the data back if needed. Clearing data is also the common protocol for a system that is in active use like an IIS (e.g., deleting a patient record – see Data Retention and Destruction).

Purge – A data "purge," or secure erase, renders recovery of the data infeasible using commercial tools or lab techniques – ultimately it is no longer possible to make sense of the data. There are many ways to accomplish this process, but the most common method is to use specific overwriting techniques to overwrite the data and drives (e.g., 0s and 1s overwritten seven times). This can be done by using commercial products (e.g., BC Wipe), but some platforms already include these tools. Purging should always be done at the admin level (DBA) so a user does not accidently erase/overwrite viable data. This process should only be used to destroy/remove data when it is no longer needed – e.g., pulling a disk or repurposing a server.

Destroy – The final level of security is to "destroy" the actual device that contains the data by using a method that results in complete physical destruction. Common methods include shredding, burning, or smelting. The system "owner" with operational/financial responsibility should ultimately oversee this process (authorize, account for, and verify). Any removal of hardware should be documented and follow a strict chain of custody. If using a third party to destroy the hardware, the IIS administrator should receive a copy of the certificate of destruction.

[57] http://www.intel.com/content/dam/www/public/us/en/documents/guides/server-refresh-planning-guide.pdf

IIS administrators are encouraged to become familiar with existing IT policies and procedures for hardware management and cleansing. The Clear, Purge, and Destroy concepts should be applied to all paper, portable devices (laptops, thumb/storage drives, tapes), and physical hardware (servers, hard drives) that contain PHI and ePHI.

NOTE: Hard drives contained within printers should also be subject to the same protocols as other hardware and portable devices. If reports containing patient level data have been printed on the machine, the data can potentially be retrieved and reproduced from the hard drive.

The following links include additional information on hardware management and data removal:

- Guidelines for Media Sanitization (NIST SP 800-88 rev 1)[58]
- HIPAA remote use guidance[59]
- Your Mobile Device and Health Information Privacy and Security[60]

Conversation Starters:

- ➔ Does the jurisdiction have existing IT policies around hardware management? Do these policies extend to portable media? Does the jurisdiction have existing policies around the use of personal devices for accessing or storing ePHI?
- ➔ Does the IT or IIS Program keep a log of hardware assets used in conjunction with the IIS? Does this log track the final disposition of the hardware (e.g., returned, transferred, stolen, destroyed)?
- ➔ What polies/procedures exist for the purging of data or destruction of hardware where ePHI may have been stored?

[58] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[59] http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

[60] https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Facility, Workforce and Contracted Security Considerations

Facility and workforce security policies encompass all the security considerations around the physical building and areas were the IIS infrastructure is housed and the general hiring/contracting practices for the IIS workforce. This includes the policies and procedures around appropriate employee access to hardware, systems, and ePHI, as well as security training, managing changes in roles or employment status, and sanctions against employees who fail to comply with security policies and procedures. These policies also pertain to the BAAs and SLAs with contracted service providers.

Facility Security:

Facility-level security may be outside of the direct control the IIS, but IIS administrators should be familiar with the policies and procedures in place for securing the building and the specific areas (server room/data center) where the IIS infrastructure is housed. This includes considerations such as who has access, how access is granted/revoked, how physical access is monitored or logged, how protections are maintained/ensured, etc. If existing policies and procedures are inadequate, IIS administrators should work with the necessary entities to ensure that IIS infrastructure is properly secured.

Conversation Starters:

- ➔ How is general access to the building/facility managed? Is the access protocol different for employees versus building support staff (e.g., janitorial, maintenance)? If the building is open to the public, how is visitor access managed and monitored?
- ➔ What restrictions are in place for managing access to the specific area(s) where the IIS infrastructure resides? Is the access protocol different for IT/IIS administrators, general employees, and building support staff (e.g., janitorial, maintenance)?
- ➔ What physical safeguards are in place for IIS infrastructure (e.g., door locks with keypad or ID scan, locked server racks, security cameras, surge protectors)? Does the facility have a backup power source in case of a power outage? Are the physical safeguards adequate, or do they need improvement?
- ➔ Is a log maintained to track access to the area where the IIS infrastructure resides (written or electronic)? Who monitors these logs? How often are they reviewed?
- ➔ What is the protocol for retracting access if/when access is revoked or no longer necessary? What happens to the keys, key codes, ID badges, etc. to ensure that access by the individual is no longer permitted?
- ➔ Is a log maintained of any physical modifications that may impact the area where the IIS infrastructure resides (e.g., building modifications such as movement of walls, lock changes or rekeying, electrical changes or repair, internet cable service/repair)?
- ➔ Is a log maintained of the physical movement of IIS hardware to/from the designated space, specifically the removal of old hardware, who performed the removal, when the removal was performed, and the final disposition of the hardware and any data it may have contained?

Workforce Security (Human Resources):

Like facility and data center security, many elements of workforce security may be outside of the direct control of IIS administrators. While many workforce security functions fall under the purview of Human Resources, IIS administrators should be familiar with the policies and procedures in place for hiring new employees who will have access to IIS data or infrastructure (e.g., immunization program and IT staff). This may include verifying identity and even performing background checks when the level of access may deem it appropriate. It also includes standard practices around terminations and resignations where system access should be revoked. If existing policies and procedures are inadequate, IIS administrators should work with Human Resource administrators to revise these policies as needed.

From an IIS perspective, most access to the IIS can be restricted through user agreements, issuance of appropriate logon credentials, and limiting access through system-based user roles and permissions (see User Management). Back-end support access is generally managed by IT administrators and/or application vendors. All employees (or business associates) that will be administering or accessing IIS data or infrastructure should be familiar with all applicable security policies and procedures. This can be accomplished through:

- New employee training
- Refresher training for existing employees on a routine basis and/or whenever policies or procedures have been revised
- Easily accessible documentation of existing policies and procedures
- Routine review of user access with modifications as needed, including termination of access
- Sanctions for users who violate security policies and procedures

The following document contains additional information on workforce threats and considerations for the development of workforce policies and procedures around ePHI access: Do You Know Who Your Employees Are?[61]

Conversation Starters:

- ➔ What are the current hiring policies/protocols for individuals who will have a high level of access to IIS infrastructure and ePHI?
- ➔ What is the protocol for retracting access if/when access is revoked or no longer necessary?
- ➔ Do training modules/programs exist for raising general security awareness? Is there specific training for administrative staff and IIS program staff regarding documented IIS security policies and procedures?
- ➔ What happens to staff who knowingly or inadvertently trigger a security incident?

[61] http://www.hhs.gov/sites/default/files/Cyber-awareness-monthly-issue-7.pdf

Contracted Services/External Hosting:

Whether a contracted partner is providing hosting infrastructure or human support services, these partners must still comply with jurisdictional security requirements for the protection of the IIS and related ePHI. The terms of these arrangements are often detailed in BAAs and SLAs that are administered and overseen by IIS and/or IT administrators. Even under these contracted arrangements, access to the IIS and ePHI should be restricted based on appropriate role-based need and job function.

Many states/jurisdictions have been moving towards centralized IT support models in an attempt to maximize shrinking budgets and consolidate resources. This trend has led many IIS to experience a series of challenges including decreased response time for resolving technical issues, lack of IIS-specific knowledge among members of the IT pool, and difficultly procuring necessary IIS hardware/support tools. As a result of this move towards centralized IT and as general budgeting challenges persist, external IIS hosting has become increasingly common. Virtual server environments like those offered by Amazon Web Services (AWS), Microsoft Azure Cloud, and physical server farms like those offered by some IIS vendors offer a reasonable and cost-effective alternative to IIS programs. These external hosting models often transfer the responsibility for server/platform management and support to an external entity while still allowing the IIS to maintain control of their own database and front-end operations.

Essentially, the hosting service may assume some or all the roles traditionally performed by an IT administrator: facility and data center security, workforce security, hardware maintenance and network protections, platform and third-party software version updates, virus/malware protection, encryption, data backup management, breach detection (intrusion detection and prevention), contingency planning, and failover management. While many hosting environments have participated in security audits and have been certified at a Department of Defense level of security in accordance with NIST and ISO standards, the IIS should still be a diligent partner to ensure the protection of the IIS and ePHI to the extent possible.

Details of the hosting relationship are often spelled out in the BAA and/or SLA, where terms and conditions are defined. IIS administrators should identify who within their organization is responsible for overseeing performance of the BAA/SLA and signing/negotiating renewals. IIS administrators should be familiar with what services are (and are not) provided under the BAA/SLA, what technical controls the host has in place to address IIS security threats, and whom the IIS administrator should contact if they have questions/concerns or need assistance. The IIS administrator should also find out if the vendor has a cyber insurance policy and what the policy covers in case a cyber event should occur.

Conversation Starters:

- ➔ What are the terms of the BAA? What are the terms of the SLA?
- ➔ How is the actual data in the IIS protected with external hosting?
- ➔ Is the IIS being hosted on an individual/private server/cloud or one shared with other clients or applications? (Best Practice: An IIS should be hosted on its own environment to prevent any cascading activity that may be generated by a breach or cyber attack.)
- ➔ Is the Cloud environment hosted in the U.S. or overseas? If overseas, how is the sovereignty and protection of the IIS data guaranteed? Does jurisdictional law/policy prohibit overseas hosting/support? If so, is that explicitly stated in the BAA/SLA?
- ➔ Are there specific points of contact identified with the hosting service/vendor? Do the contacts vary during an emergency response or 24/7 scenario?
- ➔ Who is ultimately responsible for overseeing performance of the BAA and SLA? Who is ultimately responsible for managing the renewal of these agreements?

Security Maintenance Routines

Even in the absence of a security event, IIS administrators and staff should actively observe and apply good security practices. Security should be more than simple theory; it should be integrated into standing daily, weekly, monthly, and annual maintenance routines. Examples include reviewing and updating plans and relevant documentation, providing general security awareness training to staff and system users, and making documentation accessible to staff with specific operational and response duties. IIS programs should commit adequate time and resources to Prepare, Plan, Document, and Test for various IIS security situations.

Prepare – Performing a Risk Assessment is the best method to prepare for a security event. By documenting all people, workflows, data flows, and supporting processes involved with the IIS, followed by identification of all known threats and possible fail points, the appropriate administrative and technical controls can be implemented to the extent possible. The Risk Assessment should be reviewed/updated on an annual basis to ensure that it continues to support evolving threats and technologies.

Plan – Administrative controls (policies and procedures) and technical controls (hardware and software security tools) provide the first layer of security planning by addressing known vulnerabilities. If or when these controls fail, appropriate Response Planning and Contingency Planning ensure that access to the IIS is maintained or restored as quickly as possible.

Document – Appropriate documentation of all IIS operations and security elements should be maintained, updated on a regular basis, reviewed with staff through routine tabletops/training, and stored where it can be easily accessed by appropriate staff. Certain routine processes should also be documented, such as data backups, archiving activities, hardware movement, etc., where a paper trail may be necessary and relevant. Finally, documenting an actual security event is critical and provides a written record of the nature of the event and the various elements of the resolution effort.

Test – Testing of plans and technical controls should be performed on an ongoing, routine basis to ensure that all vulnerabilities have been addressed and that the controls that have been put in place perform as intended. The fundamental goal of any testing activity is to practice the documented procedures and identify and resolve weaknesses in the security solution.

Note: As previously noted, the ultimate test for any security solution is penetration testing, which involves hiring a certified expert to identify vulnerabilities in a security solution. A penetration test may also result in damage to the IIS or loss of data, so IIS that participate in a penetration test should be prepared to do a ground-up rebuild if needed (see Contingency Planning).

Chapter 5: Conclusion

IIS administrators should use this document as a resource to meaningfully engage in conversations about IIS security with their IT and vendor support staff. IIS administrators should take an active role in risk assessment activities and ensure that proper administrative and technical controls are in place to support the prevention, detection, response, and recovery from known security threats and vulnerabilities. Because threats, technologies, and security standards evolve rapidly, IIS staff should not assume that current security measures remain adequate or appropriate. Security management should be an active and ongoing practice that is incorporated into all areas of IIS routine operations.

As threats and vulnerabilities are identified, IIS administrators should be prepared to accept, prevent, eliminate, or transfer the risk. Documentation should be created and maintained on a routine basis, and policies and procedures should be strengthened as needed to support evolving security strategies. Security tools, procedures, and plans should be regularly tested through tabletop exercises and/or active functional tests to ensure that the IIS is properly positioned to manage a physical or cyber attack.

Chapter 6: Appendices

Appendix A. Glossary of Terms

Key Players:

Database Administrator – Technical position responsible for the creation, maintenance, backups, querying, tuning, administrative user assignment, and security of an organization's databases.[62]

IIS Administrators – Collective term to include IIS managers, IIS staff, and immunization program managers

IIS Manager – Oversees the day-to-day programmatic operations of the IIS.

IIS Staff – Under the supervision of the IIS Manager, assists with overseeing the day-to-day programmatic operations of the IIS.

Immunization Program Manager – Oversees the day-to-day programmatic operations of the Immunization Program. This position may or may not supervise the IIS Manager.

IT Manager – Oversees the day-to-day technical infrastructure of an agency. This position may or may not supervise the IIS Manager.

IT Staff – Under the supervision of the IT Manager, assists with overseeing the day-to-day technical infrastructure of an agency.

Owner/Operator – Person or entity that is ultimately responsible or accountable for making legal, business and operational decisions about the IIS. Where this responsibility resides may vary by jurisdiction.

Records Management Specialist – Administrative position responsible for managing information for the organization including identifying, classifying, storing, securing, retrieving, tracking, and destroying or permanently preserving records.[63]

Security Officer – Administrative position responsible for overseeing the development and implementation of security policies and programs for the mitigation or reduction of security threats/vulnerabilities and to ensure compliance with federal, state, and local security laws and policies.

Vendor – An external IIS product developer and service provider. Responsible for technical development and code maintenance and upgrades. In some cases, may provide additional support services such as hosting, DBA, and help desk support.

[62] https://www.techopedia.com/definition/1187/database-administrator-dba

[63] https://en.wikipedia.org/wiki/Records_management

Other Terms:

Business Associate (BA) – HIPAA term. A business associate (BA) is a person or entity that performs certain functions "on behalf of" a CE including the use, disclosure, or creation of PHI.[64]

Business Associate Agreement (BAA) – HIPAA term. A contract between a HIPAA-covered entity (CE) and a HIPAA business associate (BA) that contains assurances for the safeguarding of PHI by the BA.[65]

Covered Entity (CE) – HIPAA term that applies to healthcare providers, insurers, and clearinghouses that transmit standard electronic transactions (CEs or CE). If a state agency fits the definition of a CE under HIPAA, HIPAA rules apply to the state agency; however, many state agencies that house an IIS are not considered CEs because the agency does not provide, bill, or receive payment for healthcare services, or the agency been designated a "hybrid entity" to exclude the IIS as a HIPAA-covered activity.[66]

Electronic PHI (ePHI) – electronically stored or transmitted PHI.

Health Level 7 (HL7) – Messaging standard used for exchanging electronic health records. Supports a variety of message types, including VXU (Unsolicited Vaccination Record Update), QBP (Query by Parameter), and Response (RSP).

High-Risk/High-Value Data Elements – In relation to IIS and PHI, this term refers to data elements that can be used in whole or in part for criminal activity, such as financial fraud, identify theft, or person locator activities. These data elements may include usernames, passwords, names, addresses, SSN, mother's maiden name, addresses, etc.

Protected Health Information (PHI) – Personal information that can be used in whole or in part to identify a specific individual (name, date of birth, address, medical record details, etc.). For HIPAA purposes, the term applies to any individually identifiable information that is held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral.[67]

Service Level Agreement (SLA) – An official contract between a service provider and a customer that details the nature, quality, and scope of the services to be provided.[68]

[64] http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf

[65] Idem.

[66] Idem.

[67] Idem.

[68] http://www.businessdictionary.com/definition/service-level-agreement.html

Appendix B. Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
AHIMA	American Health Information Management Association
AWS	Amazon Web Services
BAA	Business Associates Agreement
BAs	Business Associates
CDC	Centers for Disease Control and Prevention
CEs	Covered Entities
CSF	Common Security Framework (CSF)
DBA	Database Administrator
DDoS	Distributed Denial of Service
DHHS	Department of Health and Human Services
DMZ	Demilitarized Zone
DOB	Date of Birth
EHR	Electronic Health Record
EOC	Emergency Operations Center
ePHI	Electronic Protected Health Information
FAR	Federal Acquisition Regulation (FAR) RMF
FIPS	Federal Information Processing Standard
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance (HITRUST)
HL7	Health Level Seven
HTTPS	Hypertext Transfer Protocol Secure or HTTP with TLS
IIS	Immunization Information Systems
IISSB	IIS Support Branch
ISO	International Organization for Standardization
IT	Information Technology
MFT	Managed File Transfer
NASCIO	National Association of State Chief Information Officers
NCIRD	National Center for Immunization and Respiratory Diseases
NIST	National Institute of Standards and Technology
OS	Operating System
OCR	Office of Civil Rights
OGC	Office of the General Counsel
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
PKI	Public Key Infrastructure
RMF	Risk Management Framework
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SRA	Security Risk Assessment
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Social Security Number
TLS	Transport Layer Security
UI	User Interface
VLAN	Virtual Local Area Network

Appendix C. References and Suggested Reading

Advanced Encryption Standard (technical standards): http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

AHIMA Retention and Destruction of Health Information: http://library.ahima.org/doc?oid=107114#.WKnmgzvyuUk

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (NIST 800-66 r1):
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf

Breaches Affecting 500 or More Individuals: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Confidentiality and Privacy Considerations for IIS: http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf

Contingency Planning Guide for Federal Information Systems (NIST 800-34 r1):
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Digital Identity Guidelines DRAFT (NIST 800-63-3) New: https://pages.nist.gov/800-63-3/sp800-63-3.html

Do You Know Who Your Employees Are?: http://www.hhs.gov/sites/default/files/Cyber-awareness-monthly-issue-7.pdf

Electronic Authentication Guideline (NIST 800-63-2) Retiring:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Fact Sheet: Ransomware and HIPAA: http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Guide for Conducting Risk Assessments (NIST 800-30 r1): http://csrc.nist.gov/publications/PubsSPs.html#SP 800

Guide for Cybersecurity Event Recovery (NIST 800-184):
http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf

Guide to Enterprise Password Management (Draft) (NIST 800-118) Historical:
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Guide to Intrusion Detection and Prevention Systems (IDPS) DRAFT (NIST 800-94 r1):
http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

Guide to Malware Incident Prevention and Handling for Desktops and Laptops (NIST 800-83 r1):
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (NIST 800-122):
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Guidelines for Media Sanitization (NIST SP 800-88 rev 1):
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

HIPAA Breach Notification Rule: https://www.hhs.gov/hipaa/for-professionals/breach-notification/

HIPAA remote use guidance:
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

HIPAA Security Rule – Part 164, Subpart C:
https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164-subpartC.pdf

HIPAA Security Series (topic 2) – Administrative Safeguards:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es

HIPAA Security Series (topic 3) – Physical Safeguards:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf?language=es

HIPAA Security Series (topic 4) – Technical Safeguards:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es

HIPAA Security Series (topic 5) – Organizational, Policies and Procedures and Documentation Requirements:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf?language=es

HIPAA Security Series (topic 6) – Basics of Risk Analysis and Risk Management:
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

IIS Functional Standards 2018-2022: https://www.cdc.gov/vaccines/programs/iis/func-stds.html

McAfee Labs 2017 Threats Predictions: https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

Medical Record Retention and Media Formats for Medical Records:
https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/SE1022.pdf

NIST HIPAA Security Rule Toolkit: https://scap.nist.gov/hipaa/

NIST Special Publications (SP 800): http://csrc.nist.gov/publications/PubsSPs.html

OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

ONC Health IT Guide to Privacy and Security of Electronic Health Information:
https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171 r1):
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf (simplified version of NIST 800-53)

Public Key Infrastructure (technical standards):
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

Secure Hash Algorithm (technical standards): http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html

Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53 r4):
http://csrc.nist.gov/publications/PubsSPs.html#SP 800 (see simplified version – NIST 800-171)

Security Risk Assessment Tool: https://www.healthit.gov/providers-professionals/security-risk-assessment

Security Rule Guidance Material: http://www.hhs.gov/hipaa/for-professionals/security/guidance/

State Cybersecurity Resource Guide:
https://nascio.org/Publications/ArtMID/485/ArticleID/435/State-Cybersecurity-Resource-Guide

State Medical Record Laws: https://www.healthit.gov/sites/default/files/appa7-1.pdf

Transport Layer Security (technical standards): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Your Mobile Device and Health Information Privacy and Security:
https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Appendix D. Conversation Starters Quick Reference

Prevention: Network and System Protections

- ➔ What network security protections does the organization currently have in place to secure the IIS? Does the IIS operate in a DMZ or VLAN? Is the IIS protected by intrusion detection and intrusion prevention tools? Who is responsible for overseeing and maintaining network security?
- ➔ What system-level security protections does the organization currently have in place to secure the IIS? Are firewalls enabled for the Operating System and/or Web Application? Is the server protected by an anti-virus software?
- ➔ Are there requirements for IIS users to maintain active anti-virus and anti-spyware software on their workstations or other tools used to access the IIS?
- ➔ What policies and procedures are in place to manage routine system patches for operating systems and third-party support tools? Is a log maintained to document when a patch has been applied and who performed the update?
- ➔ Has penetration testing, a network vulnerability scan, and/or a web application scan been performed in relation to IIS security? If so, when was the last test/scan performed, and/or how often are these activities performed?

Prevention: Data Protections/Encryption

- ➔ Does the IIS reside on its own server? Is the server hosted in-house or with an external third party?
- ➔ Does the IIS encrypt data at rest? If so, what is being encrypted (server, database, or specific fields)? What version of encryption is being applied? If no encryption is being applied, is the IIS willing to accept related risks identified during the Risk Assessment?
- ➔ Does the IIS encrypt data in transit? If so, what protocols/versions does the IIS support?
- ➔ What ePHI does the IIS store? Is there other "high value" data produced by or stored in the IIS? Would these high-value data elements benefit from additional security (e.g., hashing)?
- ➔ Do the existing levels of protection seem appropriate, or do they need to be reassessed? If not already protected, would ePHI or high-value data benefit from encryption?
- ➔ Does the organization have existing policies around the encryption of workstations, laptops, and/or portable storage devices?

Prevention: User/Account Management

- ➔ What policies or procedures does the IIS program have in place to ensure that each user has their own individual login credentials? What happens if it is determined that a user account is being shared among multiple users?
- ➔ What features does the IIS have in place to restrict user access based on job function and duties? What processes are in place to review role assignments in the IIS to ensure that they remain current and appropriate to the user? How is this process managed for administrative level users?
- ➔ What are the current password requirements configured in the IIS? Do they follow industry best practices for strong passwords? Do passwords expire? If so, how often and can a previously used password be recycled?
- ➔ What happens to a user account after multiple failed login attempts? How many attempts are allowed? Does the IIS have a "forgot username/forgot password" feature? If so, what tools are used to verify the user and reissue credentials?
- ➔ Does the IIS support automatic timeout following a period of inactivity? Does the IIS allow a user to be logged on in more than one session simultaneously?
- ➔ What policies and procedures does the IIS program have in place for reviewing inactive user accounts? Is there a feature to disable account access? What is the process for reactivating a disabled user account?
- ➔ What audit logs does the IIS have in place for monitoring user access, access attempts, and user activity during an active session?

- Is there a routine process for reviewing and updating language in User and Site Level Agreements? Is there a process for having users and sites renew their agreements on a routine basis? Does the IIS offer security training or educational materials in conjunction with granting or renewing user access?

Prevention: Electronic Communications

- What electronic communications does the IIS generate? Are the messages generalized or patient specific?
- Does the program have a process (manual and/or automated) in place to identify and deactivate bad contact information?
- Does the IIS send reports that contain patient detail by email?
- Does the IIS log all events (e.g., electronic communications, reports) in which a patient is specifically identified?

Prevention: HL7 QBP Security Considerations

- Does the IIS offer HL7 QBP/RSP support?
- What data elements are providers required to submit in the QBP?
- What data does the IIS return in the RSP? How are high-risk data elements handled in the RSP? Are they mirrored, stripped, or updated? Is the IIS supplying any information in the RSP that the submitter didn't already supply in the QBP?
- What match criteria is the IIS using? Does the submitter receive any feedback on what did/did not match?
- Are there changes that need to be made to IIS features/functionality or policies/procedures for the support of HL7 QBP/RSP?

Detection: General

- Does the organization leverage an intrusion detection and alerting tool? Does the monitoring include IIS activity or just network activity? What tool(s) is/are being used, and what activity is being monitored? Can additional activities be added to those currently monitored?
- Who receives the intrusion alerts? What is the protocol for performing further investigation and notifying other key players? Is instruction detection paired with intrusion prevention?
- What audit logs does the IIS have in place for monitoring user access, access attempts, and user activity during an active session? Is there a process for reviewing these on a routine basis?
- Is there a procedure that users should follow if they identify records that don't seem quite right?
- What policies and procedures does the IIS program have in place for investigating and addressing suspicious activity?

Response: Response Planning

- Does the IIS have a formal written Response Plan? Is the plan customized to the IIS? What type of events does the plan cover? Does the plan include components for (1) detection/ investigation, (2) contingency/emergency operations, and/or (3) recovery/restoration?
- Does the Response Plan include a full list of key contacts including roles, responsibilities, and contact information?
- How often are the plan and contact information reviewed and updated?

Response: Contingency Planning

- Does the IIS have a formal written Contingency Plan? Is the plan customized to the IIS?
- Does the plan include a full list of key contacts including roles, responsibilities, and contact information?
- Does the plan include multiple layers of contingency in case the previous layer fails?
- How often are the plan and contact information reviewed and updated? How often is the plan tested?
- Does the IIS have a failover environment or hot site? How far away is the failover environment from the primary instance of the IIS? Does the failover/hot site have a power generator?
- How closely does the security infrastructure for the failover mirror that of the primary instance? Is it possible to participate in a site visit or security audit of this location?

- ➔ Is the changeover manual or automatic? If manual, how quickly can the failover be brought on line? How often is the data in the failover environment refreshed? How often is this procedure tested?
- ➔ What is the IIS program's maximum threshold for downtime (no access or severely restricted access) before alternative data collection methods are implemented? Does this policy apply only to statewide/jurisdiction-wide outages or also localized outages?
- ➔ Does the IIS have a standalone version of the application that can be used remotely? If so, how is this standalone version accessed/distributed? What is the chain of custody for devices used to collect data? What is the process/procedure for getting the data back into the IIS? What is the process/procedure for clearing data from the devices used for collection?
- ➔ What is the policy/procedure for data entry when users have to resort to paper-based data collection?

Response: Attack Mitigation

- ➔ Does the organization leverage an intrusion detection and prevention tool? What tool is being used? What activities is the intrusion prevention tool configured to respond to, and what actions does it take?
- ➔ When an intrusion is prevented, how is the IT and/or IIS Program notified? Who is notified? What are the policies/procedures for investigating and responding to an event notification?
- ➔ If an intrusion is discovered through a report from a user or through the routine review of audit logs, does the IIS have a formal written policy/procedure for how to investigate, report, and respond to a possible incident? What actions can be taken by staff to prevent further damage?

Response: Breach Notification

- ➔ Does the IIS have a documented policy/procedure for investigating a possible breach that involves patient records?
- ➔ Does the IIS include tools that can identify patients who have been added, modified, deleted, or viewed during a specific time frame or by a specific user or IP address?
- ➔ Does the IIS Program have a written policy/procedure for notifying patients when there is evidence that their record may have been compromised in some way? Does the policy apply differently if the compromised records were obtained through the user interface, a stolen device, or from paper records?

Recovery: Data/Database Backup Procedures and Restoration

- ➔ Does the IIS have documented procedures for IIS data, database, and server backups – who oversees this process, what data is backed up, how this process occurs (tools used), how often this process occurs, where backups are stored, how long backups are stored?
- ➔ What security mechanisms are in place for protecting the backed-up data?
- ➔ What is the extent of data loss that the IIS Program is willing to accept in the scenario that the IIS system or database must be restored from a backup file?
- ➔ Is there a documented routine for reviewing backup files for content? Is there a testing protocol for ensuring that the system can be restored from the backup files?

Administrative Policies and Routines: Hardware Management

- ➔ Does the jurisdiction have existing IT policies around hardware management? Do these policies extend to portable media? Does the jurisdiction have existing policies around the use of personal devices for accessing or storing ePHI?
- ➔ Does the IT or IIS Program keep a log of hardware assets used in conjunction with the IIS? Does this log track the final disposition of the hardware (e.g., returned, transferred, stolen, destroyed)?
- ➔ What polies/procedures exist for the purging of data or destruction of hardware where ePHI may have been stored?

Administrative Policies and Routines: Facility Security

- How is general access to the building/facility managed? Is the access protocol different for employees versus building support staff (e.g., janitorial, maintenance)? If the building is open to the public, how is visitor access managed and monitored?
- What restrictions are in place for managing access to the specific area(s) where the IIS infrastructure resides? Is the access protocol different for IT/IIS administrators, general employees, and building support staff (e.g., janitorial, maintenance)?
- What physical safeguards are in place for IIS infrastructure (e.g., door locks with keypad or ID scan, locked server racks, security cameras, surge protectors)? Does the facility have a backup power source in case of a power outage? Are the physical safeguards adequate, or do they need improvement?
- Is a log maintained to track access to the area where the IIS infrastructure resides (written or electronic)? Who monitors these logs? How often are they reviewed?
- What is the protocol for retracting access if/when access is revoked or no longer necessary? What happens to the keys, key codes, ID badges, etc. to ensure that access by the individual is no longer permitted?
- Is a log maintained of any physical modifications that may impact the area where the IIS infrastructure resides (e.g., building modifications such as movement of walls, lock changes or rekeying, electrical changes or repair, internet cable service/repair)?
- Is a log maintained of the physical movement of IIS hardware to/from the designated space, specifically the removal of old hardware, who performed the removal, when the removal was performed, and the final disposition of the hardware and any data it may have contained?

Administrative Policies and Routines: Workforce Security

- What are the current hiring policies/protocols for individuals who will have a high level of access to IIS infrastructure and ePHI?
- What is the protocol for retracting access if/when access is revoked or no longer necessary?
- Do training modules/programs exist for raising general security awareness? Is there specific training for administrative staff and IIS program staff regarding documented IIS security policies and procedures?
- What happens to staff who knowingly or inadvertently trigger a security incident?

Administrative Policies and Routines: Contracted Services/External Hosting

- What are the terms of the BAA? What are the terms of the SLA?
- How is the actual data in the IIS protected with external hosting?
- Is the IIS being hosted on an individual/private server/cloud or one shared with other clients or applications? (Best Practice: An IIS should be hosted on its own environment to prevent any cascading activity that may be generated by a breach or cyber attack.)
- Is the Cloud environment hosted in the U.S. or overseas? If overseas, how is the sovereignty and protection of the IIS data guaranteed? Does jurisdictional law/policy prohibit overseas hosting/support? If so, is that explicitly stated in the BAA/SLA?
- Are there specific points of contact identified with the hosting service/vendor? Do the contacts vary during an emergency response or 24/7 scenario?
- Who is ultimately responsible for overseeing performance of the BAA and SLA? Who is ultimately responsible for managing the renewal of these agreements?

Appendix E. HIPAA Appendix A to Subpart C of Part 164 – Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Healthcare Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Reuse (R)
		Accountability (A)
		Data Backup and Storage (A)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

Appendix F. Potential IIS Security Threats and Vulnerabilities (Examples)

Category	Possible Threats
Facility (Building/Server Room)	■ Natural disaster, fire, acts of war, vandalism ■ Unauthorized access to the building or server room ■ Facility maintenance or renovation ■ Power outage/power surge
Employees/Administrators	■ Inappropriate access privileges/permissions ■ Malicious employees ■ Careless employees ■ Staff turnover
Network	■ Network outage (e.g., web server) ■ Denial of Service (DoS) attack ■ Malicious software (e.g., ransomware) ■ Hackers (hobby or professional)/targeted attack ■ Zero Day Vulnerabilities (operating system or support apps) ■ Attack on another system in the same network
IIS Hardware	■ Theft, vandalism ■ Removal/replacement ■ Incorrect configurations ■ Hardware failure
IIS Software	■ Malicious software/spyware ■ Coding vulnerabilities ■ Incorrect configurations
IIS Access	■ Unauthorized access using a valid user account (hackers, sharing of accounts, etc.) ■ Inappropriate access privileges/permissions ■ Staff turnover
Data in IIS	■ Hackers (hobby or professional)/targeted attack ■ Printing, transmitting, or locally storing data exported/extracted from the IIS ■ Malicious entry/removal of data ■ Accidental entry/removal of data ■ Multiple instances of the database (main, backup, failover)
External Communications (text, email)	■ Delivery to incorrect recipient ■ Messages contain ePHI/high-value data elements
User Workstations/Laptops	■ Unauthorized workstation access ■ Theft, vandalism ■ Removal/replacement ■ Incorrect configurations ■ Malicious software/spyware ■ Locally stored ePHI
External Devices (local storage, portable devices)	■ Misplacement, theft ■ Locally stored ePHI ■ Unauthorized access

http://www.immregistries.org

This document is published by American Immunization Registry Association (AIRA), an organization founded to advocate for the support of immunization information systems.