Cybersecurity Toolkit for Rural Hospitals and Clinics

April 2020

NATIONAL RURAL HEALTH RESOURCE CENTER

525 South Lake Avenue, Suite 320 | Duluth, Minnesota 55802
(218) 727-9390 | info@ruralcenter.org
Get to know us better: www.ruralcenter.org

This project is/was supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) under grant number UB1RH24206, Information Services to Rural Hospital Flexibility Program Grantees, $1,100,000 (0% financed with nongovernmental sources). This information or content and conclusions are those of the author and should not be construed as the official position or policy of, nor should any endorsements be inferred by HRSA, HHS or the U.S. Government.

This report was prepared by:

Joe Wivoda
Analysts
2400 Meadowbrook Parkway
Duluth, GA 30096
Phone: 770-493-5588
www.analysts.acsicorp.com

and

NATIONAL
RURAL HEALTH
RESOURCE CENTER

National Rural Health Resource Center
525 S Lake Ave, Suite 320
Duluth, Minnesota 55802
Phone: 218-727-9390
www.ruralcenter.org

TABLE OF CONTENTS

Introduction 3
Step One: Awareness 6
Step Two: Assessment 8
Step Three: Implementation & Remediation 10
Step Four: Education 13
Conclusion 15

INTRODUCTION

Ransomware and other cybercrime are growing threats to hospitals big and small. When Hollywood Presbyterian Hospital had their data locked by a ransomware attack that was likely initiated by an unwitting employee, they chose to pay the $17,000 ransom to get their data back. In contrast, Methodist Hospital in Henderson, Kentucky, chose to go to their backups and restore their data, avoiding paying the ransom[1]. Both hospitals were required to report the incidents as data breaches and had significant downtime during the attacks, stretching into nearly a week. These are just two examples of how ransomware is threatening hospitals and clinics today, and ransomware is only one type of cyberthreat to be aware of for hospitals and clinics of all sizes and in all geographic locations. Rural hospitals and clinics experience compounded challenges due to their small staff and lack of resources, including finances. Recognizing the need to be prepared, South Peninsula Hospital, a critical access hospital (CAH) in Homer, Alaska, has engaged senior leadership to support their prevention efforts and maintains cybersecurity as a priority for their hospital and community[2].

From December 30, 2015 to December 15, 2017, there were 392 data breach incidents reported to the US Department of Health and Human Services (HHS). These breach incidents that have affected 17,215,903 patients, and these are only the data breaches of unsecured protected health information affecting 500 or more individuals[3]. Since 2009, more than 176 million patients have had their data breached in some sense, with 132 million of those patients affected as a result of hacking or another information technology (IT) incident. Protected health information is a very valuable black-market product. A single complete medical record with personal health information (PHI), Social Security Number, health insurance information, and other details can fetch nearly $1,000. There is an evidenced need for health care organizations to do a better job of protecting their health information and information systems.

Failure to adequately protect your hospital or clinic from cyberattacks and ransomware can be quite costly. Any breach of a significant size (typically over 500 patient records) is required to be reported to the local news media as well as HHS. However, all Health Insurance Portability and Accountability

[1] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/
[2] https://www.ruralhealthinfo.org/rural-monitor/alaska-hospital-cybersecurity/
[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Act (HIPAA) covered entities and their business associates are required to provide notification following a breach of unsecured protected health information. Additionally, similar notifications of a breach on a vendors' personal health records and their third-party service providers must also be reported[4]. The damage to the organization's reputation is significant, and the financial penalties from HHS and the Office of Civil Rights (OCR) can be very large, especially if a known risk was not remediated or repeated warnings were ignored. It has been demonstrated that organizations that made good faith efforts to remediate identified risks, and who cooperate with OCR and HHS, were most likely to receive smaller fines.

Protecting your hospital, clinic or even home computers from cyber threats can be a daunting task. It involves more than installing a good antivirus package, implementing a strong firewall or modifying existing security practices to protect the digital workplace from all the cyber threats that exist, or may exist in the future. Creating awareness of such need and developing strategies to overcome the challenges that small IT staff and limited resources present for rural hospitals and clinics, can support not only rapid response to attacks, but also preparedness.

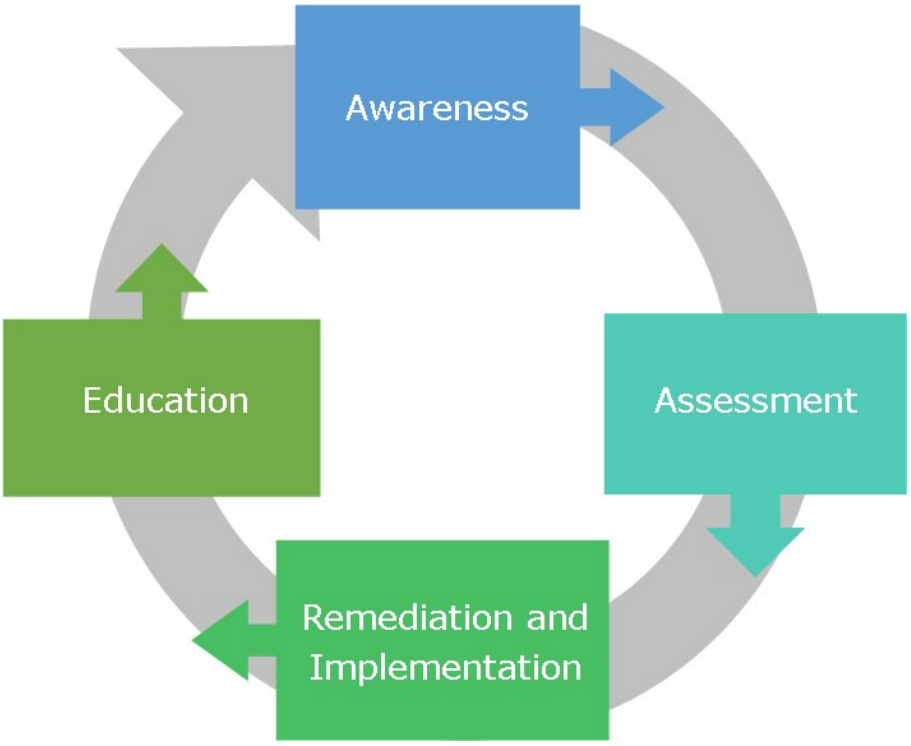
This toolkit includes a survey of available resources from various governmental and non-profit organizations. It includes checklists and tools that are appropriate for all audiences, hospitals or clinics, including those in a rural setting. Examples of included resources and tools include sophisticated and detailed risk assessment tools, board education documents, and even educational material for protecting home computers.

The very best protection your organization can have from cyber threats is to have a well-educated workforce. Helping staff, providers and leadership understand the threats, how to identify a possible breach attempt, and to be aware of risks will provide an excellent first line of cyber defense. The skills and knowledge they learn can be used at their home, protecting their family and internal networks from attack. This is important because one vector for cyberattacks is from a home user's email or compromised computer network. In small rural facilities, it is commonplace that staff support multiple roles or "wear multiple hats." As such, staff should be made aware of their responsibility in prevention and response to cybercrime in their various roles and provided the needed tools, such as those found in this

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

toolkit, for awareness, assessment, implementation and remediation, and education.

The process described in this document addresses cybersecurity through awareness, assessment, implementation and remediation, and education. Although the process is cyclical, each of these steps are important and are most effective when followed in the order listed in this document, beginning with awareness. It is not recommended to skip ahead to the risk assessment, for example, before addressing all prior steps. Education, though listed as the last step in the process, is incorporated throughout all steps.



STEP ONE: AWARENESS

The first step in building an effective cybersecurity program is awareness. The responsibility for protecting a hospital or clinic from cybercrime rests with everyone, including the board of directors, leadership, IT staff, and all other users of computing technology.

Awareness of the importance of cybersecurity can be accomplished with many techniques. Annual employee training is a great place to start, but there are many other methods as well. Occasional reminders are a great way to keep cybersecurity front-of-mind. Some hospitals use table tents in the cafeteria or small posters in the elevator or other commonly used locations. These reminders need to be simply worded and short, and some of the resources below contain examples of these tools. This is a low-cost, high-visibility opportunity to keep cybersecurity on the minds of employees and patients. A common source of data breaches is a contractor's laptop. Perhaps a contract coder or collection agency takes a copy of data with them to work on off site and the laptop is stolen or hacked into. Awareness not only needs to be built with the contractor, but also with the manager and staff that work with contractors.

Some common best practices used by hospitals and clinics to build awareness are outlined below.

Awareness

- Send reminder emails about security threats.
- Share stories and news articles of hospitals or clinics that have experienced cyber attacks.
- Place cybersecurity posters and table tents with brief, catchy reminders.
- Provide periodic cybersecurity reminders and discussion topics at board and management meetings.

Table 1. Awareness Tools and Resources

Tool	Description
Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients	HICP aims to raise awareness and provide vetted cybersecurity practices. It discusses the current cybersecurity threats facing the health care industry and sets forth a call to action. • **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations** Discusses the ten Cybersecurity Practices (herein called Practices) and Sub-Practices for small health care organizations. It is intended for IT and/or IT security professionals and serves to guide organizations on what to ask their IT and/or IT security teams or vendors
Cybersecurity Threats in Rural America: How to Protect Your CAH	Webinar by the National Rural Health Resource Center discussing cybersecurity, with a focus on the issues affecting CAHs with recommendations.
Report on Improving Cybersecurity in the Health Care Industry	Report to Congress by the Health Care Industry Cybersecurity Task Force on the state of cybersecurity in health care. Presents risks, imperatives, recommendations, action items and more, with information specific to small and rural providers.
Stay Safe Online - CEO and Board Awareness	Information on risk assessment, education, threat trends, and others. Developed by the National Cyber Security Alliance and designed for both non-technical and technical readers.
Stop. Think. Connect. Toolkit	US Department of Homeland Security (DHS) resources for cybersecurity for all segments of a community. Very complete promotional resources that are sorted by audience. Industry and Small Business toolkits will be most the useful for hospitals and clinics.
US-CERT	US Computer Emergency Readiness Team (US-CERT) website. Excellent educational material on protecting your home and work computing environments, cloud computing basics and other topics designed for a broad audience.
Health IT Playbook, Section 7: Privacy & Security	The Office of the National Coordinator for Health Information Technology (ONC) Health IT Playbook has links to many tools as well as descriptions of the issues surrounding HIPAA, cybercrime, and general network security.

STEP TWO: ASSESSMENT

Once stakeholders and staff become aware of and understand some issues around cybersecurity, the next step is to assess threats and vulnerabilities in the hospital or clinic. Too often, assessment is the first and only step that hospitals complete as part of the HIPAA Privacy and Security Risk Assessment, and it is typically handed off to the person responsible for IT. Leadership engagement in the rural facility can aid staff in moving work beyond assessment into implementation and remediation.

A privacy and security risk assessment is the primary tool for assessing cyber risks. It is always best to have a person external to the organization perform the assessment. A "second set of eyes" will identify things that are overlooked by staff. Further, a person experienced in performing risk assessments for hospitals or clinics will use their past experiences and can often make additional recommendations. If a complete risk assessment has never been done, then a reviewer external to the hospital is most important.

Hiring a consultant to perform the risk assessment can be highly beneficial but also costly for a single facility. Regional or state-based health care networks can use their scale and buying power to secure preferred pricing for each facility. Networks can coordinate skilled staff at each hospital member to perform assessments for other hospitals. This can be very effective and provides increased awareness of each facility's capabilities and skills.

Networking is an area where rural facilities excel. It is strongly suggested if your rural hospital or clinic has not explored the benefits of networking. Network benefits that are related to cybersecurity support include but are not limited to: collaborating on solutions, knowledge sharing, resource and staff sharing, group purchasing, vendor and contract negotiation, and care coordination.

From experience in the field, there are many common risks that hospitals and clinics struggle with such as inadequate backup procedures, poor employee termination procedures, and poor IT management procedures. Backups are critical to any organization and should be verified periodically and stored in a safe manner. The IT department should make a standard practice of checking server and firewall logs, looking for data breaches, hardware issues or other concerns.

One of the biggest threats and most common vulnerabilities is notification to IT of terminated employees. Even in small facilities many hospitals and clinics do not notify IT in a timely manner when employees are terminated, and yet this is a very easy fix. Human resource (HR) departments typically have a checklist for terminations which includes collecting property, keys and/or access cards, and providing the employee with their final paycheck. Simply adding a step in the process to notify IT staff to disable all accounts would mitigate this significant vulnerability.

Risk assessments are not just for IT systems. Hospitals and clinics are encouraged to assess environmental and facility risks to the organization as well. Some best practices for assessment are below.

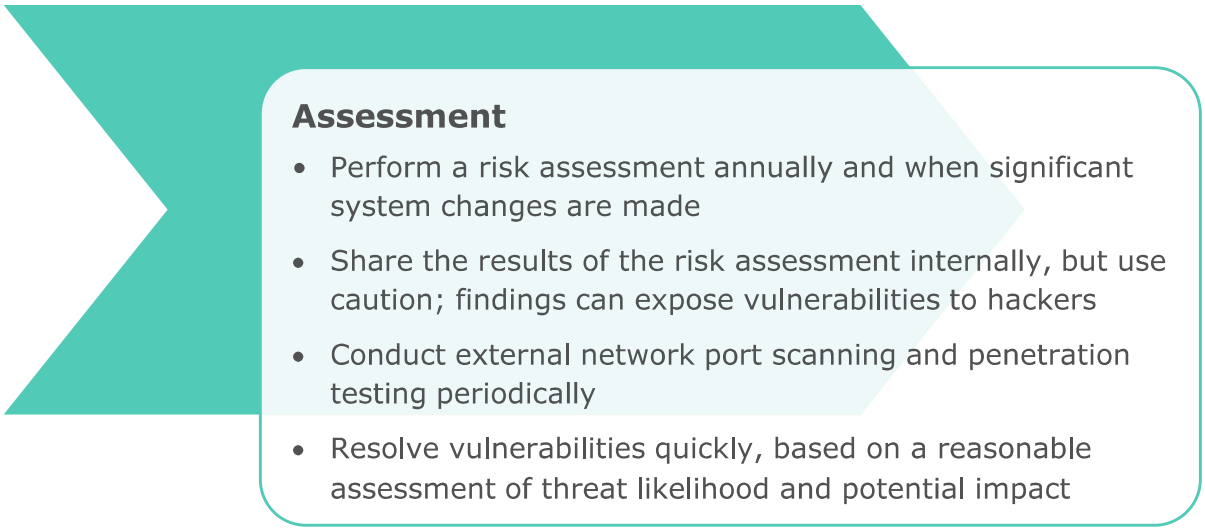


Table 2. Risk Assessment Tools and Resources

Tool	Description
Security Risk Assessment Tool	Developed by ONC, this PC/iPad app can be used to perform risk assessments required under HIPAA. Primarily for IT and security staff at the hospital or clinic.
Cybersecurity Assessment Tool	Federal Financial Institutions Examination Council (FFIEC) tool for assessing risks and preparedness. Complete and in-depth tool that is best used by IT, security, and privacy staff.
Health IT Playbook, Section 7: Privacy & Security	The ONC Health IT Playbook has descriptions and videos of the issues surrounding HIPAA risk assessment and how to protect your computer at work and at home. The videos can be useful for staff and others during training.

STEP THREE: IMPLEMENTATION & REMEDIATION

The assessment phase presents several opportunities for improvement. Risks and threats that were identified in the assessments will need to be remediated, and new processes or technologies will likely need to be implemented to protect health information.

Common risks, such as notifying IT of employee terminations, have common solutions. Reaching out to other organizations for example policies and processes on risk mitigation can help your facility learn from other's experiences. Networks, trade organizations, web resources, and peer hospitals and clinics will likely have sample policies or procedures that can help.

An important part of implementation and remediation is having a solid Incident Response Policy. This is a HIPAA requirement and is a best practice for any incident a hospital or clinic may experience, including cyber incidents[5]. The incident response process may follow Hospital Incident Command Structure (HICS) or any framework that the hospital or clinic uses for incidents[6]. It is important that the response plan include the appropriate personnel, adequate documentation, and communication, and breach notification procedures. The incident response plan should be exercised periodically in rural facilities. Some common best practices for implementation and remediation are listed on the following page.

[5] https://www.hhs.gov/hipaa/for-professionals/security/index.html
[6] https://training.fema.gov/is/courseoverview.aspx?code=is-100.hcb

Implementation & Remediation

- Review and improve HR policies to include employee sanctions for data breach.
- Assign responsibility to monitor and install software security updates.
- Implement daily server and firewall log checks.
- Centralize management of antivirus software.
- Outsource firewall management to a company that specializes in data security.
- Improve data backup process to include off-site storage, encryption, and periodic testing.
- Form an Incident Response Team to include IT, external vendors, and hospital leaders.
- Implement an Incident Response Policy that includes cyber threats.

Table 3. Implementation and Remediation Tools and Resources

Tool	Description
Cybersecurity: How a Rural Alaska Hospital is Safeguarding Its Patients' Information	This article provides an overview of cybersecurity threats and challenges faced by rural health care facilities. Describes how the IT staff at the South Peninsula Hospital, a Critical Access Hospital in Alaska, safeguards their hospital's data.
Small Firm Cybersecurity Checklist	Very complete spreadsheet from the Financial Industry Regulatory Authority (FINRA) with details that are most useful for CAH or clinic IT, security and privacy staff.
Cybersecurity Controls Checklist	Checklist for protecting your hospital or clinic from cyber threats developed by the State of Utah.
Cybersecurity Framework	Comprehensive set of tools geared towards security and IT professionals from the National Institute of Standards and Technology (NIST).
Health IT Playbook, Section 7: Privacy & Security	The ONC Health IT Playbook has links to many tools as well as descriptions of the issues surrounding HIPAA, cybercrime, and general network security.

Tool	Description
Security Risk Assessment Tool	PC/iPad app from ONC for performing risk assessments required under HIPAA. Primarily for IT and security staff at the hospital or clinic.
"Top 20" Cybersecurity Checklist	A checklist for remediating the top vulnerabilities that exist at a small practice or at home. Developed by the American Institute of Certified Public Accountants (AICPA), the information is applicable to most hospitals, clinics or home users.
Health Information Sharing and Analysis Center	Health Information Sharing and Analysis Center (H-ISAC) contains a forum and community for sharing cyber and physical security threats, best practices, and mitigation strategies.
US-CERT	Educational material from US-CERT on protecting your home and work computing environments, cloud computing basics, and other topics designed for a broad audience. Simple steps for protecting yourself from cybercrime are included.

STEP FOUR: EDUCATION

Continued education is not only a HIPAA requirement, but also a best practice for protecting hospitals and clinics from cyber threats. Education should include all stakeholders, including board members, leadership, IT staff, and frontline staff. Educational materials for home use are also included in the tool list below. Some best practices for education are listed below.

Education

- Provide cybersecurity training during annual employee education.
- Share handouts of free antivirus software for staff to take home and protect their own computers.
- Show demonstrations of what phishing emails or malicious websites look like.

Table 4. Cybersecurity Education Tools and Resources

Tool	Description
Cyber Security Guidance Material	This section of the HHS.gov website houses educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to cyber-related security incidents.
Stay Safe Online - CEO and Board Awareness	Information on risk assessment, education, threat trends, and others from the National Cyber Security Alliance, designed for both non-technical and technical readers.
Stop. Think. Connect. Toolkit	DHS resources for cybersecurity including very complete educational resources that are sorted by audience. Industry and Small Business toolkits will be most useful for hospitals and clinics.
US-CERT	US-CERT website with excellent educational material on protecting your home and work computing environments, cloud computing basics, and other topics designed for a broad audience.

Health IT Playbook, Section 7: Privacy & Security	The ONC Health IT Playbook has links to many tools as well as descriptions of the issues surrounding HIPAA, cybercrime, and general network security.
H-ISAC	Health Information Sharing and Analysis Center (H-ISAC) contains a forum and community for sharing cyber and physical security threats, best practices, and mitigation strategies.

CONCLUSION

With the rising value of protected personal health information, and new and emerging cyberattack mechanisms, cybersecurity has become a critical topic for health care in both urban and rural settings. Over 170 million breached patient accounts necessitate that hospitals and clinics need to do a much better job of keeping protected health information secure.

Much work has been done to create tools and resources that can help hospitals and clinics achieve stronger cyber systems, and rural health care organizations are not exempt. The resources listed in this toolkit are merely a sample and vary in sophistication. There are many audiences that need to be addressed for a comprehensive cybersecurity program to be effective, from board members and front-line staff to IT professionals. All audiences need to be involved and engaged to protect their organizations from growing threats. By building awareness, assessing organizational risks, implementing new policies and procedures, and educating staff, hospitals, and clinics can improve data protection and be better prepared to respond appropriately to cyber threats.