Electronic Health Network Cybersecurity Readiness Assessment

A Best Practices Review

MARYLAND
HEALTH CARE
COMMISSION

Overview

An increase in cyber threats is causing organizations in the health care industry to examine their existing cybersecurity readiness activities. Assessing cybersecurity readiness is essential to ensuring the technical infrastructure of an Electronic Health Network (EHN) is adequately protected. The Maryland Health Care Commission (MHCC) developed this *Electronic Health Network Cybersecurity Readiness Assessment* ("tool") as a way to facilitate cybersecurity awareness among EHNs operating in Maryland. The information contained in this document is aimed at providing guidance to EHNs as they develop their cybersecurity plans.

Electronic Health Network Certification and Cybersecurity Review

Maryland COMAR 10.25.07, *Certification for Electronic Health Networks and Medical Care Electronic Claims Clearinghouses,* requires payors that accept electronic health care transactions originating in Maryland to accept transactions from EHNs that obtain MHCC certification. EHNs seeking MHCC certification must obtain national accreditation through an accreditation body recognized by MHCC. EHNs must submit proof of national accreditation, including supporting documentation, such as site visit reports and policies and procedures reviewed during the site visit. **EHNs are encouraged to complete a cybersecurity readiness assessment when applying for MHCC certification; however it is not required.** The MHCC identified best practices from the NRECA Cooperative Research Network Smart Grid Demonstration Project[1] and the Department of Health and Human Resources[2]. EHNAC's criteria most closely related to the cybersecurity best practices are included for reference purposes. The illustration on the next page details how to complete the tool.

[1] NRECA Cooperative Research Network Smart Grid Demonstration Project, Guide to Developing a Cyber Security and Risk Mitigation Plan, 2011. Available here: https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf

[2] Department of Health and Human Resources, Top 10 Tips for Cybersecurity in Health Care. Available here: https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Testing and Monitoring				
Related EHNAC Criteria	**Documentation for cybersecurity best practice:**	**Implementation**		
		Fully Implemented	**Partially Implemented**	**To Be Implemented**
III. L. 5, III. L. 7, VI. B. 1	**Perform annual vulnerability assessments**			
	Candidate identifies criticality of assets	☒	☐	☐
	Candidate identifies the owners of the assets	☒	☐	☐
	Candidate identifies the frequency of scanning	☒	☐	☐
	Candidate identifies and timelines for remediation	☐	☒	☐
Overall Implementation Status of Best Practice		☒	☒	☐
Total Count of Overall Implementation Statuses		3	2	0

Cybersecurity Category being assessed

Related EHNAC criteria

Select which most accurately reflects the organization's implementation of associated procedures for the cybersecurity best practice.

Indicate the overall implementation status of the cybersecurity best practice based on the procedures that have been implemented

Indicate how many cybersecurity best practices fall into each implementation category

Description of Implementation Levels

Fully Implemented: All procedures associated with the cybersecurity best practice.

Partially Implemented: Less than 100% of procedures associated with the cybersecurity best practice.

To Be Implemented: Procedures associated with the cybersecurity best practice have not yet been implemented.

Network Protection

Related EHNAC Criteria	Best Practice	Implementation		
		Fully Implemented	Partially Implemented	To Be Implemented
II. A. 9, III. M. 1	**Wireless networks are encrypted**			
	Candidate identifies critical assets	☐	☐	☐
	Policies define access requirements	☐	☐	☐
	Candidate has defined policies for "guest access" including separate guest Wi-Fi	☐	☐	☐
	Candidate physically secures access points, such as mounting and locking the device in place	☐	☐	☐
	Candidate uses WPA2 security protocols	☐	☐	☐
	Candidate limits Wi-Fi signal to not reach beyond building	☐	☐	☐
	Candidate scans for and removes unauthorized access points on the network	☐	☐	☐
	Candidate employs a wireless intrusion prevention system	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
II. A. 6	**Up-to-date anti-virus software is used to protect system and data**			
	Anti-virus software should auto update virus signatures from the service provider as updates are available	☐	☐	☐
	A centralized server based anti-virus system should be deployed for any computer on the networked system	☐	☐	☐
	Antivirus software should be loaded onto standalone PCs and automatically enabled to check for viruses	☐	☐	☐
	Servers are checked daily for viruses	☐	☐	☐
	Workstations are checked daily for viruses	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
III. L. 1	**Up-to-date firewalls are used to protect system and data**			
	Candidate has clearly defined access polies and procedures to ensure firewalls are updated and patched on a routine basis	☐	☐	☐
	Firewalls should have rules for allowing specific traffic such as defining a source IP address (or range of addresses), defined destination IP address (or range of addresses), defined destination port (or range of ports)	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
	Identify electronic security perimeter			

III. L. 2, III. L. 5, III. L. 9	Candidate maintains list of all critical cyber assets that should be maintained within an electronic security perimeter	☐	☐	☐
	Candidate has policies and procedures to monitor updates for all software	☐	☐	☐
	Candidate uses VPN access if remote access is allowed	☐	☐	☐
	Firewalls should have rules for allowing specific traffic such as defining a source IP address (or range of addresses), defined destination IP address (or range of addresses), defined destination port (or range of ports)	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
Total Count of Overall Implementation Statuses				

Asset Identification

Related EHNAC Criteria	Best Practice	Implementation		
		Fully Implemented	Partially Implemented	To Be Implemented
VI. B. 21	**Identify and classify critical cyber assets**			
	Candidate identifies facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the system	☐	☐	☐
	Candidate has policies and procedures to identify cyber assets associated with a critical asset	☐	☐	☐
	Candidate groups cyber assets	☐	☐	☐
	Candidate has procedures to determine which cyber assets are essential	☐	☐	☐
	Candidate has procedures to identify cyber assets with qualifying connectivity	☐	☐	☐
	Candidate has policies and procedures to compile the list of critical cyber assets	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
VI. C. 7	**All devices containing PHI are inventoried and can be accounted for**			
	Candidate maintains a list of all devices containing PHI	☐	☐	☐
	Candidate maintains a log-out sheet to track which devices are assigned to which users	☐	☐	☐
	Candidate has policies and procedures in place to inventory all devices containing PHI	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
Total Count of Overall Implementation Statuses				

Testing and Monitoring				
Related EHNAC Criteria	**Best Practice**	**Implementation**		
		Fully Implemented	**Partially Implemented**	**To Be Implemented**
III. L. 5, III. L. 7, VI. B. 1	**Perform annual vulnerability assessments**			
	Candidate identifies criticality of assets	☐	☐	☐
	Candidate identifies the owners of the assets	☐	☐	☐
	Candidate identifies the frequency of scanning	☐	☐	☐
	Candidate identifies and timelines for remediation	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
III. L. 5, III. L. 7, VI. B. 1	**Perform annual risk assessment**	☐	☐	☐
	Candidate identifies and documents asset vulnerabilities	☐	☐	☐
	Candidate identifies and documents internal and external threats	☐	☐	☐
	Candidate acquires threat and vulnerability information from external sources	☐	☐	☐
	Candidate identifies potential business impacts and likelihoods	☐	☐	☐
	Candidate determines enterprise risk by reviewing threats, vulnerabilities, likelihoods and impacts	☐	☐	☐
	Candidate identifies and prioritize risk responses	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
VI. B. 22, VI. F. 4	**Routinely monitor and evaluate security controls**			
	Procedures should be aligned with candidate's business and security goals	☐	☐	☐
	Account for changes within the organization, operating environment, and implemented technologies	☐	☐	☐
	Produce sufficient evidence to illustrate continued adherence to security requirements	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
III. L. 7, III. N. 1	**Perform annual penetration testing**			
	Candidate performs both internal and external penetration testing	☐	☐	☐
	Candidate tests segmentation controls	☐	☐	☐
	Candidate identifies all critical systems to be tested	☐	☐	☐
	Candidate tests authentication rules	☐	☐	☐
	Candidate tests any critical applications, such as payment or web applications	☐	☐	☐
	Candidate has social engineering tests performed	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
Total Count of Overall Implementation Statuses				

Network Access				
Related EHNAC Criteria	**Best Practice**	**Implementation**		
		Fully Implemented	**Partially Implemented**	**To Be Implemented**
II.A.3, VI. B. 5, VI. B. 6	**All authorized users have access to only the information they need to perform their duties (least-privileges access)**			
	Candidate should have policies and procedures in place to determine what access users need to complete their duties	☐	☐	☐
	Candidate should have policies and procedures to review user access routinely to verify that users are still assigned least privileges access	☐	☐	☐
	Candidate should have policies and procedures to remove or change privileges when an employee changes positions or leaves the organization	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
VI. D. 1	**Network access is restricted to authorized users and devices**			
	Candidate must implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.	☐	☐	☐
	Candidate maintains a list of authorized users and/or programs	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
VI. C. 1, VI. C. 3, VI. C. 4	**Physical access to secure areas is limited to authorized individuals**			
	Locks are on and utilized on all doors leading to secure areas and cabinets housing secure information	☐	☐	☐
	Candidate maintains a list of all authorized individuals	☐	☐	☐
	Access points to secure areas are limited	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
III. M. 1	**Mobile devices are configured to prevent unauthorized use**			
	Candidate maintains list of all authorized mobile devices	☐	☐	☐
	Candidate has policies clearly defining what authorized and unauthorized use is	☐	☐	☐
	Candidate has policies and procedures to prevent installing unauthorized software or apps on mobile devices			
	Candidate requires use of strong passwords on all mobile devices	☐	☐	☐
	Candidate performs remote wipe if mobile device is reported as lost or stolen	☐	☐	☐

	Candidate performs periodic audit of security adherence and configuration	☐	☐	☐
	Internal and external memories are encrypted	☐	☐	☐
	VPN is required for mobile device to access the network	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
Total Count of Overall Implementation Statuses				

Personnel

Related EHNAC Criteria	Best Practice	Implementation		
		Fully Implemented	Partially Implemented	To Be Implemented
V. B. 4, VI. B. 4	**Assign responsibility for security risk management to senior level manager**			
	Candidate provides a list of individuals, who are responsible for HIPAA compliance including the protection of electronic PHI and the list includes at least 1 senior level manager.	☐	☐	☐
	Candidate provides a list of privacy and security officials, which are senior level management, and their back-ups.	☐	☐	☐
	Candidate describes roles and responsibilities for privacy and security officials.	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
V. B. 2, V. B. 3, VI. B. 12	**Staff is trained, at least annually, on how to recognize symptoms of viruses or malware of computers and how to avoid virus/malware infections**			
	Candidate should provide cyber security training upon hire and an annual refresher	☐	☐	☐
	Training programs should require staff to attest that the information was both delivered and understood	☐	☐	☐
	Candidate should have procedures to document all personnel that have completed training	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
Total Count of Overall Implementation Statuses				

Computer Security

Related EHNAC Criteria	Best Practice	Implementation		
		Fully Implemented	Partially Implemented	To Be Implemented

III. L. 8	**Computers contain no peer-to-peer applications**			
	Candidate has policies in place to deter using peer-to-peer applications	☐	☐	☐
	Candidate has policies and procedures in place to check for peer-to-peer applications and remove if necessary	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
II. A. 2	**Public instant messaging, such as gchat, services are not used**			
	Candidate has policies in place to deter using public instant messaging applications	☐	☐	☐
	Candidate has policies and procedures in place to check for public instant messaging services and remove if necessary	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
II. A. 2	**Private instant messaging services, if used, are secured appropriately**			
	Private instant messaging provides encryption of data during transit	☐	☐	☐
	Policies and procedures exist to verify the identity of the sender and recipient	☐	☐	☐
	Private instant messaging secures/encrypts past messages so that they cannot be accessed by non-authorized users	☐	☐	☐
Overall Implementation Status of Best Practice		☐	☐	☐
Total Count of Overall Implementation Statuses				

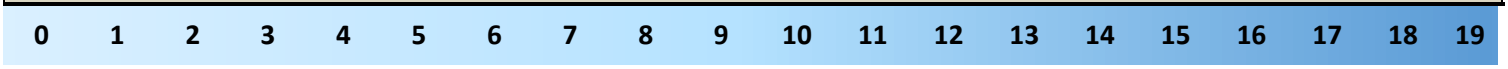
Rating Scale

Determine your score by adding the total number of best practices that are fully implemented, partially implemented, or to be implemented, using the following weights: fully implemented – 1; partially implemented .5; and to be implemented 0. Add all of the scores together to arrive at your total score.

Add scores for "Fully Implemented," "Partially Implemented," and "To Be Implemented."

Fully Implemented Score		Partially Implemented Score		To Be Implemented Score		Total
5	+	(10*.5)	+	(3*0)	=	10

Best Practices Indicator – Implementation Scale



Partial **Moderate** **Advanced**

Best Practices Indicator Descriptions

Partial: Minimal development of formal processes and diffusion of cybersecurity practices throughout the organization (6 and below).

Moderate: Some formalized processes are established and diffused throughout the organization. Processes are being developed to address identified gaps (7-12).

Advanced: Formalized organization-wide processes to address the majority of cybersecurity risks are in place and diffused throughout the organization (13-19.)

About MHCC

The Maryland Health Care Commission (MHCC) is an independent regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policy makers, purchasers, providers and the public. The MHCC is responsible for advancing health information technology statewide and fostering innovation in a way that balances the need for information sharing with the need for strong privacy and security policies.

Resources

1. *NRECA Cooperative Research Network Smart Grid Demonstration Project, Guide to Developing a Cyber Security and Risk Mitigation Plan, 2011. Available here: https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf*
2. *Department of Health and Human Resources, Top 10 Tips for Cybersecurity in Health Care. Available here: https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf*
3. *Network Computing, 8 WLAN security best practices, 2016. Available here: http://www.networkcomputing.com/network-security/8-wlan-security-best-practices/1977586091*
4. *North American Electric Reliability Corporation, Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, 2010. Available here:* http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf
5. *Irfahn Khimji, Vulnerability Management Program Best Practices—Part 3, 2016. Available here: http://www.tripwire.com/state-of-security/vulnerability-management/vulnerability-management-program-best-practices-part-3/*
6. *Security Magazine, Best Practices for Conducting a Cyber Risk Assessment, 2015. Available here: http://www.securitymagazine.com/articles/86754-best-practices-for-conducting-a-cyber-risk-assessment*
7. *PCI Security Standards Council, Best Practices for Maintaining PCI DSS Compliance, 2014, Available here: https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf*
8. *Rackspace, Best Practices for firewall rules configuration, 2016. Available here: https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration/*
9. *National Computer Board, Guideline on Information Security Policy, 2011. Available here: http://cert-mu.govmu.org/English/Documents/Guidelines/2010/Anti%20Virus%20Best%20Practices.pdf*
10. *SANS Institute, Implementing Least Privilege at your Enterprise, 2003. Available here: https://www.sans.org/reading-room/whitepapers/bestprac/implementing-privilege-enterprise-1188*
11. *Electronic Health Network Accreditation Commission Criteria, 2016. Available here: https://www.ehnac.org/program-criteria/*
12. *CIO, Secure Locations-Protection at a price, 2007. Available here: http://www.cio.com.au/article/198920/secure_locations/?pp=2*
13. *IOActive, A Risk-based Approach to Determining Electronic Security Perimeters and Critical Cyber Assets, 2009. Available here: http://www.ioactive.com/pdfs/ARisk-basedApproachToDeterminingESPsAndCCAs.pdf*
14. *Security Week, Four Tips for Designing a Secure Network Perimeter, 2013. Available here: http://www.securityweek.com/four-tips-designing-secure-network-perimeter*
15. *Computer Weekly, Best practices for enterprise mobile device security, 2016. Available here: http://www.computerweekly.com/tip/Best-practices-for-enterprise-mobile-device-security*
16. *Electronic Frontier Foundation, Secure Messaging Scorecard, 2016. Available here: https://www.eff.org/node/82654*

Glossary of Terms:

1. **Asset:** Property owned by an organization that is regarded as having value.
2. **Cybersecurity:** The technologies, processes, and practices that are designed to protect the cyber environment of an organization's critical infrastructure.
3. **Electronic Security Perimeter:** The logical border surrounding a network to which critical cyber assets are connected and for which access is controlled.
4. **Inventory:** A complete list of all physical devices, systems, and software that are owned and operated by the organization.
5. **Peer-to-Peer Applications:** Computing or networking application architecture that partitions tasks or workloads between peers who are equally privileged.
6. **Penetration Testing:** The practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
7. **Risk Assessment:** The practice of identifying gaps in an organizations critical areas and to determine actions to close those gaps.
8. **Security Controls:** Technical and administrative safeguards or countermeasures to avoid, detect, counteract, or minimize cybersecurity risks to information, computer systems, or other assets.
9. **Segmentation Controls:** The act of splitting a computer network into subnetworks, each being a network segment, to improve security by mitigating the impact of a network intrusion.
10. **VPN Access:** Access through means of a virtual private network. A virtual private network (VPN) is a network that is constructed using public wires — usually the Internet — to connect to a private network, such as a company's internal network. There are a number of systems that enable you to create networks using the Internet as the medium for transporting data.
11. **Vulnerability Assessment:** A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.