Remote Access Policy – XYZ Health Care Provider

Introduction[1]

The connected nature of today's digital landscape provides numerous opportunities to us as a healthcare provider. However, accompanying those opportunities are numerous risks. As an organization responsible for the health of our patients, we are committed to securing information and systems related to our clients, employees, stakeholders, partners, and community.

As representatives of XYZ Health Care Provider, your participation in helping keep XYZ Health Care Provider's information systems secure is of utmost importance. Knowing, understanding, and adhering to these policies as stated is a mandatory responsibility.

The Remote Access Policy is organized by sections with the following headers: Policy Goals/Objectives, Scope, Standards, Procedures, Guidelines, Policy Exemptions, Administrative Notations, Policy Definitions, Version Control, Policy Enforcement Clause, Acknowledgements, and References. These sections build upon each other to form the entirety of the policy.

In the case of situations arising, in which policy adherence may not be technically feasible or justified, an exemption may be granted. Requests consisting of justification and benefits of exemption must be made in advance and in writing to the Chief Security Officer. Failure to do so will be considered a violation of policy.

Violation of this policy is subject to disciplinary action as determined by relevant authorities. This action may include, but is not limited to, termination for employees or contractors, dismissal for non-paid staff, and the right to pursue civil or criminal prosecution.

I thank you for your support and compliance in keeping our information systems secure.

Policy Goals/Objectives

The purpose of this Remote Access Policy is to define and outline the conditions and requirements for connecting to XYZ Healthcare Provider's information systems from any external host. These objectives and goals are intended to mitigate XYZ Healthcare Provider from damages that may arise from unauthorized use of its information systems.

- To demonstrate its commitment to the security of its digital assets and infrastructure
- To define rules and conditions for proper remote access through the public Internet
- To meet regulatory requirements
- To inform users of the necessity of Remote Access Policy compliance
- To mitigate risks, threats, and vulnerabilities that arise from remote access to information systems
- To assist in quantifying risk management and assessment
- To inform users of monitoring and logging of remote access

[1] Format credit to Greene Chapter 2, "In Practice: Introduction"

Scope

This policy applies to all people or entities employed by, in contract with, or otherwise representing XYZ Healthcare Provider. It applies to remote access connections to XYZ Healthcare Provider information systems at any and all locations and branches. It includes, but is not limited to, systems necessary for online access of patients' medical records. Remote access by SSL VPN is covered by this policy. Logging and monitoring of all remote access connections is expected.

Standards

These standards are designed to establish regulatory compliance of HIPAA, HIPAA Security Rule, HIPAA Privacy Rule, HITECH Act, and Omnibus Rule. Technological standards are based on NIST publications SP 800-122, SP 800-666, SP 800-111, SP 800-52, and SP 800-113.

- All remote access connection and attempts will be logged and monitored.
- Passwords must satisfy the Password Policy, i.e. be a minimum of 8 characters and consist of symbols and upper- and lower-case letters.
    - Account lockouts will occur after three incorrectly entered passwords
- Remote and mobile workers must use multi-factor authentication when remotely accessing resources
- Mobile/Laptops/Desktops must have full-disk encryption and remote wipe capabilities
- Mobile/Laptops/Desktops must be up-to-date on patches and have working AV
- All connections must be made using SSL VPN with recommended practices as stated by NIST SP 800-113
    - TLS 1.0 or later
    - Users will undergo host integrity check prior to first login to ensure minimum security baseline
- Users must not make connections to other entities or sites while connected to XYZ Healthcare Providers by VPN.
    - For additional acceptable uses measure, refer to the Acceptable Use Policy
- Unless otherwise instructed, ePHI must not be downloaded or copied to host computer.
    - If instructed all ePHI and PII must be encrypted and securely stored at rest.

Procedures

This policy will be implemented organization wide through a training program scheduled by department leaders. Personnel from Information Technology will lead the training. Training will consist of step-by-step instructions for installation of VPN software for both mobile and desktop devices. A demonstration of the dangers of failure to properly use a SSL VPN to securely connect will also be conducted.

Remote and mobile employees will be sent recorded video lectures of the training program administered to on-site XYZ Healthcare Provider personnel. Remote and mobile employees must complete an online assessment of the training material before remote access will be allowed.

Guidelines

- Any individual with any concerns regarding how to properly adhere to the policy is welcome to contact Information Technology or their department head.
- If in any doubt about the security of a connection, it is better to err on the side of caution and not connect.
- In the event of issues arising when implementing required technological standards on a personal computer, XYZ Healthcare Provider can provide company-owned laptops if the issue cannot be resolved.

Policy Exceptions

Exemptions may be granted on a per request basis for situations where policy adherence is not feasible or justified. Requests consisting of justification and benefits of exemption must be made in advance and in writing to the Chief Security Officer. Failure to do so will be considered a violation of policy.

Administrative Notations

Lead Author	C. Ferris, Chief Security Officer
Related and Corresponding Documents	Acceptable Use Policy Acceptable Encryption Policy Password Policy
Regulatory Cross Reference	HIPAA and all addendums HITECH Omnibus Rule
Considerations and Notes	Employees should have a basis of understanding of how a VPN protects traffic. Furthermore, this policy will need to be monitored and updated immediately in the event of vulnerabilities discovered in procedure or encryption protocols.
Next Revision	01/01/2021
Policy Location	www.xyzhealthcare.org/policies/remote_access_policy.pdf

Policy Definitions

- PII – personally identifiable information
- PHI – protected health information
- ePHI – electronic protected health information
- VPN – virtual private network, a means of securing communications between two systems
- Host – the computer that the user is currently using
- SSL – Secure Sockets Layer, a symmetric-key cryptographic protocol for secure communications over computer networks, the predecessor to TLS

- TLS – Transport Layer Security, an updated version of SSL, and a symmetric-key cryptographic protocol for secure communications over computer networks
- HIPAA – Health Insurance Portability and Accountability Act of 1996, a regulatory component of the health care industry
- HIPPA Privacy Rule – the Standards for Privacy of Individually Identifiable Health Information sets limits and conditions on the use and disclosure of patient information and applies to all formats of PHI
- HIPAA Security Rule – the Security Standards for the Protection of Electronic Protected Health Information requires technical and nontechnical safeguards to protect electronic health information.
- HITECH Act – the Health Information Technology for Economic and Clinical Health Act expands the scope and requirements of the HIPAA Security Rule
- Omnibus Rule – finalizes various rules introduced in prior legislature, and establishes government authority to enforce HIPAA regulations
- NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- NIST SP 800-66 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security
- NIST SP 800-111 – Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-52 - Guidelines for Selection and Use of Transport Layer Security (TLS) Implementation
- NIST SP 800-113 – Guide to SSL VPNS

Version Control

V.	Editor	Purpose	Change Description	Authorized By	Effective Date
1.0	C. Ferris, CSO		Original	Sr. management committee	01/01/2020

Policy Enforcement Clause

Failure to comply with this policy is subject to disciplinary action as determined by relevant authorities. This action may include, but is not limited to, termination for employees or contractors, dismissal for non-paid staff, and the right to pursue civil or criminal prosecution.

Acknowledgement

I acknowledge and understand the Remote Access Policy and Acceptable Use Policy for XYZ Healthcare Provider. I hereby agree to comply with the policies in their entirety, understand and accept the enforcement clauses, and know that I can at any point ask for clarification from a department head or Information Technology regarding policy specific questions.

Employee Signature: _____

Employee Name _____

Date: _____

References

Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2008, July). *SP 800-113: Guid to SSL VPNS*. Retrieved from NIST Computer Security Resource Center: https://csrc.nist.gov/publications/detail/sp/800-113/final

Green, S., & Santos, O. (2018). *Developing Cybersecurity Programs and Policies* (3rd ed.). Pearson. doi:9780134858623

Information Security Policy Templates. (2015, April). Retrieved from SANS.org: https://www.sans.org/security-resources/policies/network-security

Johnson, R. (2014). *Security Policies and Implementations Issues* (2nd ed.). Jones & Bartlett Learning. doi:9781284056006

Office for Civil Rights. (2013, July 26). *Summary of the HIPAA Security Rule*. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Olenski, J. (2016, July 07). *SSL vs. TLS - What's the Difference*. Retrieved from GlobalSign: https://www.globalsign.com/en/blog/ssl-vs-tls-difference/

Remote Access Policy. (2005, July 19). Retrieved from Network Intrastructure and Control Systems - Appalachain State University: https://nics.appstate.edu/standards/remote-access-policy

Security Rule Guidance Material - Remote Use.pdf. (n.d.). Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Snell, E. (2015, March 20). *Breaking Down HIPAA: Health Data Encryption Requirements*. Retrieved from Health IT Security: https://healthitsecurity.com/news/breaking-down-hipaa-health-data-encryption-requirements