SECURITY STANDARDS

for Access to
PCHP Systems, including the Services and Information,
under the Information Access & Security Agreement

Adopted by PCHP: January 20, 2022

These Security Standards are policies, procedures, and guidelines governing administrative, technical, and physical matters, adopted by PCHP and as amended and in force from time to time, to govern your access to and use of the Services (including your access to any PCHP Systems and the Platform or any Platform Tools) and/or the Information, particularly as it relates to protecting certain health information that is held or transferred in electronic form, especially to assure the confidentiality, integrity, and availability of electronic-PHI. These Security Standards are incorporated in the Information Access & Security Agreement ("***Security Agreement***") between Piedmont Community Health Plan, Inc. ("***PCHP***", "***we***" or "***us***") and the health care provider ("***Provider***" or "***you***") that contracts with us or otherwise provides health care services to patients who are our Members.

1. *Definitions*: The following terms shall have the following meanings:

    a. "***Information Security Event***" is an unexplained or unexpected activity that indicates the security of a Provider System or remote access to a PCHP System may have been breached or compromised. An Information Security Event indicates that an information security policy may have been violated or a safeguard may have failed.

    b. "***Malware***" means (i) any code, program, or sub-program whose knowing or intended purpose is to damage or interfere with the operation of the software or computer system containing the code, program or sub-program, or to halt, disable or interfere with the operation of the software, code, program, or sub-program, itself, (ii) any device, method, or token that permits any person to circumvent the normal security of the software or the system containing the code, or (iii) any code, program, or sub-program whose knowing or intended purpose is to serve as an adaptive threat by, among other possibilities, obtaining and sending data from the software or computer system containing the code, program or sub-program.

    c. "***Portable Devices***" means portable computers, personal digital assistants, smartphones, tablets, MP3 devices, USB devices, SSDs, or any other portable devices that may be used for processing data.

    d. "***Provider Location***" means a physical location occupied or controlled by Provider.

    "***Services***", "***Information***", "***Users***" and all other capitalized terms used but not otherwise defined in these Security Standards shall have the meanings set forth in the Security Agreement.

2. *Information Security Program*: Provider shall implement and maintain an information security program that establishes roles and responsibilities for information security and supports the confidentiality, integrity, and availability of Provider Systems and the Information.

3. *Security Policy and Security Awareness Training*: Provider shall maintain information security policies that define requirements for access control, application and system development, passwords, remote access, data classification, operational security, network security, and physical security. Provider shall review its information security policies at least annually, or when significant changes to the environment occur, to ensure their continuing suitability, adequacy, and effectiveness. Provider shall require that all new Users complete security awareness training. Provider shall require all Users to participate in annual training.

4. *Asset Inventory*: Provider shall maintain an inventory of Provider Systems and media containing Information or otherwise used to access the Services.

5. *Acceptable Use*: Provider shall maintain and enforce security policies for the acceptable use of the Services and Information consistent with the uses permitted in the Security Agreement.

6. *Portable Devices*: Provider shall require encryption and technical controls for any User's use of Portable Devices.

7. *Protection of Data at Rest*: Provider shall protect data at rest in compliance with applicable laws, including regulatory requirements and standards.

8. *Encryption of Data*: Provider shall encrypt the following categories of data in electronic form using an encryption mechanism that conforms to Federal Information Processing Standard (FIPS) 140-2: (a) any Information that is removed from any Provider Location or any Information stored off-site; (b) any Information that is transmitted wirelessly over an untrusted connection, or over a "public network" (*e.g.*, the Internet); and (c) Portable Devices.

9. *Encryption Keys*: All keys used by Provider for encryption will be required to be handled in accordance with Provider's documented key management policies, standards, and procedures.

10. *Secure Areas*: Provider shall secure all areas that house Provider Systems, or media containing Information, by the use of appropriate physical security controls in order to ensure that only authorized Users will be allowed access and to prevent damage and interference. Notwithstanding the foregoing, with respect to Provider Systems that are not located at a Provider Location, the requirements of this Section 10 shall be deemed met by Provider's use of industry standard security measures including locking, encryption, frequent password changes, and 2-factor authentication, as applicable.

11. *Security Perimeter*: Provider shall control and restrict access to Provider Locations by use of a defined security perimeter, appropriate security barriers, entry controls, and authentication controls. Provider shall securely maintain a record of all accesses.

12. *Physical Media Controls*: Provider shall physically secure and maintain control over all paper, electronic media, and devices that contain, transmit, or display Information.

13. *Protection Against Malicious Code*: Provider has implemented and will maintain detection, prevention, and recovery controls to protect against Malware. Provider shall require all Users to be trained to prevent and detect Malware.

14. *Anti-Malware Mechanisms*: Provider shall require that anti-Malware mechanisms are deployed on all Provider Systems that are commonly affected by Malware (e.g. PCs, portable computers, and servers) and are capable of detecting, removing, and protecting against Malware. Provider shall require such anti-Malware mechanisms to be current, actively running, monitored, and capable of generating audit logs, and that definition files will be updated when they become available.

15. *Media Handling*: Provider shall protect against unauthorized access or misuse of Information contained on electronic and non-electronic media, as well as control distribution.

16. *Media and Information Disposal*: Provider shall securely and safely dispose of media (including but not limited to hard copies, disks, SSDs, CDs, DVDs, optical disks, USB devices, backup media, and hard drives) containing Information when no longer required.

17. *Monitoring*: To protect against unauthorized access or use of Information residing on Provider Systems, Provider shall:

    a. Employ essential current industry practice security controls and tools to monitor Provider Systems and log key events such as user activities (including root or administrative access), exceptions, successful and unsuccessful logins, access to audit logs, unauthorized information processing activities, suspicious activities, and Information Security Events;

b. Regularly back up Information activity logs to a secure central location, protected against tampering and unauthorized access;

c. Retain Information activity logs in accordance with regulatory requirements and best industry practices;

d. Perform regular, routine log reviews and take necessary actions to protect against unauthorized access or misuse of Information;

e. Comply with all applicable laws and regulations, including regulatory requirements, and prevailing industry practices related to monitoring and logging activities;

f. Require that the clocks of all relevant Provider Systems be synchronized using an authoritative national or international time source;

g. Incorporate date and time stamp into log entries; and

h. Employ, monitor, and keep up to date intrusion detection systems and intrusion prevention systems to monitor all network traffic and alert Users or other personnel to suspected Information Security Events.

18. *User Access Management*:

    a. To protect against unauthorized access or misuse of Information residing on Provider Systems, Provider shall employ a formal user registration and de-registration procedure for granting and revoking access and access rights to all Users.

    b. Provider shall require that all access for former users is revoked in a timely manner. Removal of access includes assurance that there are no shared accounts, including administrator and server level accounts, which have passwords that are known by former Users.

19. *Session Timeouts*: To protect against unauthorized access or misuse of Information residing on Provider Systems, Provider shall:

    a. Require that inactive User sessions be terminated or require the User to re-authenticate after a defined period of inactivity;

    b. Require that desktop, laptops and, where technically possible, servers, invoke a password-protected screen saver after a predetermined period of inactivity not to exceed 15 minutes; and

    c. Require handheld devices employ a “lock screen” security control, requiring the entry of a pass-code to unlock, after a predetermined period of inactivity.

20. *Operating System Access Control*: To protect against unauthorized access or misuse of Information residing on Provider Systems, Provider shall require that access to operating systems be controlled by a secure logon procedure with username and complex password credentials at a minimum. Provider shall require that staff, including supervisory Users, not share log-on IDs or passwords.

21. *Mobile Computing and Remote Working:* To protect Information residing on Provider Systems from the risks inherent in mobile computing and remote working, Provider shall:

    a. Identify and mitigate risks to Information from mobile computing and remote working through such control mechanisms as authenticated, encrypted VPN access, and standard, secure client device configuration requirements;

    b. Maintain and enforce policy and procedures for managing mobile and remote users; and

    c. Restrict access to the Services, PCHP Systems, or Information from any location outside of the United States or any of its territories or possessions.

22. *Configuration Standards*: Provider shall develop security standards for system components and technology frameworks to provide that there is a minimum set of security baseline requirements in place, consistent with industry-accepted system hardening benchmarks.

23. *Patch Management*: Provider shall employ a process to review and implement security patches for vendor software and firmware vulnerabilities using an established industry, risk-based framework such as a Common Vulnerabilities and Exposures (CVE) approach.

24. *Vulnerability Management*: Provider shall employ a commercially reasonable process for vulnerability management, based on the size and sophistication of Provider.

25. *Development Processes*: Provider shall incorporate security into the development lifecycle, including:

    a. Restricting access to source code to authorized Users who have a direct need to know; and

    b. Employing oversight quality controls and security management of software development.

26. *Incident Response Plan*: Provider will utilize a commercially reasonable incident response plan, based on the size and sophistication of Provider, which may include designating representatives of Provider for incident response, categorization of incidents, and responsibility for receiving alerts and investigations.

27. *Incident Training*: With respect to all Users using Provider Systems or having remote access to PCHP Systems, Provider shall train them to report any Information Security Events of which they become aware.

28. *Termination of Security Events*: Provider shall use commercially reasonable efforts to immediately address Information Security Events. Provider shall not allow any Information Security Event that it is reasonably able to terminate to persist except as required by law or regulation, or as deemed reasonably necessary by Provider to determine the identity of the perpetrator.

29. *Incorporated into Security Agreement*: These Security Standards form a part of and are hereby incorporated into the Security Agreement.