


**COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES
POLICY AND PROCEDURE MANUAL**

SUBJECT: HIPAA - Perimeter, Remote Access and Wireless Security	POLICY NO: 01-295
SECTION: Administration	EFFECTIVE DATE: 6-10-16
REFERENCE: 45 C.F.R. Subtitle A, Subchapter C, Part 164	PAGE: 1 of 6 SUPERSEDES: New Policy
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	APPROVED BY: 

PURPOSE: The purpose of this policy is to ensure there is a secure perimeter surrounding an internal network that is not directly exposed to unauthorized connections.

NOTES: ICBHS network consists of two firewalls that are used to separate and enforce limits on transactions between the internal network (trusted) and the Internet (untrusted). The Systems Information Analyst is responsible for the installation and configuration of remote access. Current ICBHS firewalls are appropriately secured to prevent unauthorized access and protect confidentiality of data accessed by authorized remote users.

DEFINITIONS: **Perimeter Devices:** Devices that pass data between the internal network and the internet or other untrusted devices. Perimeter protection includes denying transit of data except those explicitly permitted by the perimeter device configuration. Wireless access is excluded as ICBHS does not provide this functionality. ICBHS staff are prohibited to connect to outside wireless providers unless provided prior authorization by management and given pre-approved access to use

encrypted Virtual Private Network (VPN) by Information Systems BHM. Similarly remote access using an authorized, encrypted VPN may be considered part of the trusted network.

Remote Access: Remote users, who include Information Systems and Systems Information staff, are only permitted to connect to secure network resources where an approved VPN (Virtual Private Network) connection has been established using encryption and bidirectional authentication. Remote users will use the Remote Desktop Connection application only while the remote user is conducting business. It may not be used for personal use and must be automatically disconnected if unused for more than the maximum time specified in the standards. Remote access connection logs are tracked by the Systems Technology analyst within the administrative functionality of application. Users of VPN access must be approved and authorized according to the Access Control Policy. Remote access to the VPN must be initiated from ICBHS owned systems that meet the standards of the PHI Protection Policy and are secured with storage encryption, anti-virus/spyware/spam software and up-to-date security patches. Contractors and other entities may use their personal devices and equipment only when approved by Systems Technology Analyst of ICBHS. Remote access users must complete Security Awareness training prior to accessing ICBHS electronic health record system and must meet all standards of the HIPAA PHI Protection Policy.

Wireless: Wireless technology is not permitted within the networks of ICBHS. Wireless access shall be provided and installed in approved devices via Verizon USB Stick or "AirCard" and its reliability is dependent on cell signal strength.

Remote User: A user that is not directly connected to the secure local network operated by approved business associates.

Internal Wireless Network: A network that is connected directly to the corporate network without passing through a firewall. This type of network is not used within ICBHS.

External Wireless Network: A network that is connected to the internet and cannot access the internal network without traversing a firewall. ICBHS staff are prohibited to connect to outside wireless providers unless provided prior authorization by management and given pre-approved access to use VPN.

Wireless Access Point: A fixed device installed in a network so that wireless computing devices (laptops, tables, printers, etc.) can establish communications access to a local network. Wireless access points are not used in ICBHS.

Signature Update: is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity).

POLICY OWNER: Security Officer

POLICY: ICBHS adheres to the following standards to ensure there is a secure perimeter surrounding an internal network that is not directly exposed to unauthorized connections:

1. Architecture

Perimeter Architecture

Each perimeter device must enforce access control using rules that deny by default. A firewall must separate the untrusted Internet from the trusted internal network. All fixed devices including workstations, servers, printers, networked medical devices, etc. maintained by County of Imperial Information Technical

Services and maybe maintained by Systems Technology technicians or Analyst and must be on the trusted side of the firewall. Untrusted devices shall not be directly connected to the internal network.

Remote Access Architecture

In order to control access to the network, remote access gateways must be located at a chokepoint that can be controlled and monitored by Systems Technology Analyst. Remote access gateways are centralized on a firewall DMZ for control and monitoring by Systems Technology Analyst.

2. Configuration

Failed Login Attempts

Remote access systems shall be configured to allow a maximum of three consecutive failed authentication attempts. After three failed login attempts, the account will be disabled and require a requested administrative reset. Re-establishment of access privileges must follow approved processes and may include a review of system log files to identify if the authentication failures were the result of user error or an attempt to gain unauthorized access to ICBHS information assets.

Minimum requirements for systems or devices used to access the VPN:

- ICBHS issued equipment that is inspected for security during the annual Asset Inventory.
- Up-to-date anti-virus engine and signature updates.
- Current operating system and application security patches.

VPN solution requirements:

- ICBHS uses the Cisco System VPN that is an encrypted application used for remote access to protect the data from tampering, theft and session hijacking as well as from confidentiality attacks. \

- Timeout after 90 minutes without use.

3. Process

Remote Access:

- ICBHS staff are provided with a user name that is recognized by the network as soon as it is created.
- To connect remotely staff accessed the VPN client, they enter their domain credentials and access is provided.
- The VPN software is configured to only accept networks named users for ICBHS and as it recognizes the users it allows them to enter into the network.
- Business Associates must submit requests for remote access on behalf of non-employees to the Information Systems BHM.

Responsibilities of users of remote access

- Locate their devices so as to prevent unauthorized users from seeing ePHI.
- Protect all passwords and tokens to prevent unauthorized access of VPN services.
- Ensure that no ePHI is shared with unauthorized persons.
- Review on a regular basis.

Related Policies and Regulations:

Policies:

1. 01-232 HIPAA PHI Protection Policy
2. 01-231 HIPAA User Access Management Policy
3. 01-290 HIPAA Security Management Policy

Regulations:

1. 45 C.F.R. § 164.312 (a)(1): Standard: Access control.
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software

programs that have been granted access rights as specified in §164.308(a)(4).

2. 45 C.F.R. § 164.312 (a)(2)(iii): Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
3. 45 C.F.R. § 164.312 (a)(2)(iv): Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
4. 45 C.F.R. § 164.312 (b): Standard: Audit controls. Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
5. 45 C.F.R. § 164.312 (d): Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
6. 45 C.F.R. § 164.312 (e)(1): Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being.
7. 45 C.F.R. § 164.310 (b): Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.