REMOTE ACCESS TO ELECTRONIC PROTECTED HEALTH INFORMATION

Dr. _____

Changes in HIPAA requirements by the federal government include strict guidelines for remote access to protected health information (PHI) and electronic protected health information (EPHI). For protection of the physicians and their staff and the protected health information of their patients and to be in compliance with the new guidelines, we have updated our HIPAA policy and procedure for remote access.

Here is the policy:

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the information owner (physician) or his/her designated representative. If authorized, the organization:

1. Authorizes remote access to the information system only to those approved for remote access and only through the use of corporate recognized IP address and approved product *(GoToMyPC)* connecting with the host computer using completely private data stream encrypted end-to-end with 128-bit Advanced

There are costs associated with adherence to these requirements. Using "GoToMyPC, if we change application, the fee will change.

- **$75.00 one-time setup fee 1st computer. Subsequent setup per computer $50.00.**
- **$78.00 monthly fee per license. (Pass through, subject to change)**

The exposure: As a ProHealth doctor, you have access not only to your own patients but to all demographic information for all ProHealth patients in the ProHealth database including HIPPA protected information such as diagnosis' as well as critical identity theft information such as Social Security numbers. While this information is safe when you are accessing it in CareTracker, if you move any data out of CareTracker it is no longer protected by their firewall and encryption. Breaches of this information could result in significant **fines and penalties against you** from Federal Agencies. For example, HIPPA breaches can carry a fine of minimum **$100.00 per violation for each patient file breached** and the **total fines can easily be in the hundreds of thousands of dollars or an annual maximum of $1.5 million**. **There are hundreds of thousands of ProHealth patients' information in CareTracker, not just your patients' information but all physicians in ProHealth.**

You Recently requested remote access for your employee :

We strongly recommend that your employee have a Static IP so that the internet connection to all patient and financial information is more secure.

We ask that you sign below as authorization and acknowledgment that you understand the above and accept responsibility for any breach of protected information and any fines and/or penalties imposed and all legal fees. Access will not be granted without your signature. HIPAA guidelines as documented in our HIPAA Policies and Procedures Manual are attached.

_____ _____

Signature Date

Dr. _____

ProHealth Partners/Argus Medical Management HIPAA Privacy & Security Policies & Procedures Manual

S – 1031 Remote Access Control

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the information owner (physician) or his/her designated representative. If authorized, the organization:

1. Authorizes remote access to the information system only to those approved for remote access and only through the use of corporate recognized IP address and approved product *(GoToMyPC)* connecting with the host computer using completely private data stream encrypted end-to-end with 128-bit Advanced Encryption Standard (AES).

a. Documents allowed methods of remote access to the information system;
b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
c. Monitors for unauthorized remote access to the information system;
e. Enforces requirements for remote connections to the information system.

Implementation Standard(s)

This control requires explicit authorization prior to allowing remote access to HIPAA protected information. Remote access is any access to an information system by an authorized user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. **Enforcing access restrictions associated with remote connections is accomplished by control through the Security Systems Officer and IT Security Officer.**

Assessment Procedure. Determine if:

There is appropriate prior authorization for the remote access by IP address
There is documentation of allowed methods of remote access to the information system
There are established usage restrictions and implementation guidance for each allowed remote access method.
There is monitoring for unauthorized remote access to the system
There is enforcement for remote connections to the information

Wireless Access

The organization prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the information owner or his/her designated representative. If authorized, the organization:

a. Monitors for unauthorized wireless access to the information system; and
b. Enforces requirements for wireless connections to the information system.

Implementation Standard(s)

1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:
(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);
(d) A firewall is implemented between the wireless network and the wired infrastructure; There is to be no remote access allowed to the firewall
(e) MAC address authentication is utilized;
(f) Static IP addresses, not DHCP, is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

Guidance

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.

Assessment Procedure

1. the organization establishes usage restrictions and implementation guidance for wireless access;
2. the organization monitors for unauthorized wireless access to the information system;
3. the organization authorizes wireless access to the information system prior to connection;
4. the organization enforces requirements for wireless connections to the information system.
5. the organization meets all the requirements specified in the applicable implementation standard(s).

Access Control for Mobile Devices - Staff

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to its information systems unless explicitly authorized, in writing, by the information owner or his/her designated representative. If authorized, the organization:

a. May employ an approved method of cryptography to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
b. Monitors for unauthorized connections of mobile devices to its information systems;
c. Enforces requirements for the connection of mobile devices to its information systems;
d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and

f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.