

IP ADDRESS AND MOBILE DEVICES COMPLIANCE WAIVER

Dr. _____, you are receiving this waiver because we understand that you access patient information on portable devices.

Argus Medical Management tracks all IP (**Internet Protocol**) addresses used to connect to our web-based systems. IP addresses are classified as either Static or Dynamic and identify the computer you use to access information on our web-based systems.

Static IP addresses are considered much safer: a static IP is a constant address that never changes. CareTracker can only be accessed by your staff within your office with a Static IP address. The purpose of obtaining a static IP address is to restrict your staff (or others) from accessing CareTracker outside of your office.

Dynamic IP addresses are not considered safe: a dynamic address can change and Argus can prohibit your staff from accessing CareTracker when they leave your office by restricting access to only the office IP address. For example, they cannot access CareTracker from their home or give their log-in to anyone else who can then access CareTracker from anywhere because the dynamic IP address will not match the office IP address. As a physician, we can grant you remote access for dynamic addresses but feel it extremely important that you fully understand the risks of this exposure.

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 **finances 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.**

Your IP address at your home is a Dynamic IP address: We strongly recommend that you do not move any data out of CareTracker onto your home computer, laptop or tablet at home where it will not have the encryption protection it has while in CareTracker.

Access Control for Mobile Devices – Physician(s)

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., tablet, notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). **Usage recommendations** and **implementation guidance** related to mobile devices **include**, for example,

1. Implement fundamental security controls and practices, including **passwords, virus protection, and personal firewalls on all portable devices.**
2. Configuration management.
3. Device identification and authentication.
4. **Implementation of mandatory protective software (e.g., malicious code detection, firewall).**
5. Scanning devices for malicious code.
6. **Regularly updating virus protection software.**
7. Regularly scheduled scanning for critical software updates and patches.
8. Conducting primary operating system (and possibly other resident software) integrity checks.
9. Disabling unnecessary hardware (e.g., wireless, infrared).

Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. These would provide easy access to protected data if the device were lost or stolen.

For emails sent or received (on mobile or non-mobile device) by the physician containing protected health information (PHI), the **physician should delete the PHI on the reply email and should not include two identifiers** (name and any other identifying information) **without encrypting, password protecting or sending to secure portal.**

Policies and procedures recommendations for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

We ask that you sign below as acknowledgment that you understand the above and accept responsibility for any breach of protected information accessed at your home or on mobile devices.

Signature

Date

Dr. _____