**LAPTOP, PORTABLE DEVICE, AND REMOTE USE**

**POLICY AND PROCEDURE**

To customize this template document, replace all of the text that is presented in brackets (i.e. “[” and “]”) with text that is appropriate to your organization and circumstances. Many of the procedure statements below represent “best practices” for securing mobile computing. These may not be feasible or available for your practice. Be sure this document reflects the actual practices and safeguards currently in place!

**POLICY AND PROCEDURE**

National and regional laws surrounding computer usage policies vary across locations, so there’s no standard format that fits every organization. We advise seeking legal counsel to find out what needs to be included in yours

**Organization name:**

**Purpose:** This organization considers safeguarding its electronic information protected health information, intellectual property and any patient information of paramount importance. **[Organization name]** has developed a series of HIPAA privacy and security policies and procedures as well as a series of computer and internet use policies and procedures.

Certain employees and contractors of [organization] use portable and mobile computing devices including **[Insert as applicable]**:

* laptop computers
* tablet computers
* iPad or their equivalent
* Smartphones
* Other mobile devices **[specify]**

For work related tasks while traveling or at home. This sometimes entails remote access to our networks, to our applications that create, store, maintain or transmit ePHI, or to websites that create, store, maintain or transmit ePHI.

It is the policy of **[organization]** that all remote use and/or access will be done with established security safeguards.

**Procedure:**

1. Laptops and **[insert type of device(s)-for example, “Smartphone and Tablet”]** that are assigned to individuals for remote use will be accounted for on the computer asset inventory.
2. Laptops and **[insert type of device(s)-for example, “Smartphone and Tablet”]** must be configured with the standard configuration prior to use remotely.
3. The standard laptop and if available **[insert type of device(s)-for example, “Smartphone and Tablet”]** configuration will require a unique user login ID and password complexity equal to that of the network if feasible. The current policy on password strength and change will be in force.
4. The standard laptop and **[insert type of device(s)-for example “Smartphone and Tablet”]** configuration will require the laptop to automatically log off after a period of **[enter timeout period-portable devices should have a lower timeout than devices secured in your medical practice because they are more susceptible to theft]** minutes inactivity.
5. The standard configuration will require documents to be written to the **[organization]** server where possible. **[Organization]** will use appropriate technology tools to synchronize all laptop and **[insert type of device(s)-for example, “Smartphone and Tablet”]** files with the network server and thus ensure the laptop files are a) resident on the server and b) part of the routine backup.
 **Note:** A variety of software applications ensure that data on mobile devices can be automatically synchronized to your network or cloud server-such as Dropbox, Evernote, Apple iCloud, Microsoft Office 365 or other synchronization tools and so forth.
6. The standard configuration will require network drive folder level passwords where feasible, when the files relate to confidential or proprietary information.
7. Laptops and [insert type of device(s)-for example, “Smartphone and Tablet”], will be encrypted at either the entire drive or solid-state memory level, or with a partition encryption where the partition contains ePHI.
8. Encryption keys will be separate from the device and maintained with appropriate complexity by the Security Official or their designee.
9. Screenshots with ePHI shall not be saved to laptops or **[insert type of device(s)-for example, “Smartphone and Tablet”]** unless encryption is enabled.
10. The standard configuration will require malicious software protection to be enabled on the laptop and **[insert type of device(s)-for example, “Smartphone and Tablet”],** along with automatic live updates.

**Note:** Smartphones, tablets and other mobile devices are also susceptible to viruses or spyware!
11. If laptops **[insert type of device(s)-for example, “Smartphone and Tablet”]** are used the security official will enable automatic updating of security patches.
12. When laptop or mobile device security patches or updates are not automatically downloadable but otherwise can be downloaded from a website, the security official will notify, by email, all employees who have a laptop or **[insert type of device(s)-for example, “Smartphone and Tablet”],** requesting they download and install the update. The security official will request a confirmation receipt of the email and notification of the update. The security official will track responses and if necessary take possession of the device to ensure updates.
13. **[Optional]** Laptops or **[insert type of device(s)-for example, “Smartphone and Tablet”]** will be configured with remote security controls that will remotely wipe the device upon loss or theft, scan for malware, provide GPS tracking, encrypt partitions or memory that stores ePHI, alert or block introduction of unauthorized SIM cards.
14. Smartphones and tablets that are used to access, receive or transmit ePHI via email shall only do so with this medical practice’s secure domain mail server or **[insert type of secure encrypted email system]**. Email settings shall be configured to limit the number of recent or emails stored on the device.
15. Smartphones and tablets that are used to access, receive or transmit ePHI shall be configured to limit the number of text messages stored on the device. Only secure text messaging systems shall be used.
16. Laptops or **[insert type of device(s)-for example, “Smartphone and Tablet”]** that use wireless communications including Bluetooth will be configured to always turn off the “Discoverable Mode” to ensure the device is not viewable by unauthorized persons. Alternatively, where “Discoverable Mode” is necessary for proper pairing, the user shall be trained to disable this mode when in public places where data and conversations can be discovered by nearby unauthorized individuals.
17. Laptop and **[insert type of device(s)-for example, “Smartphone and Tablet”]** users will be trained and periodically reminded to pair their devices with the pairing laptop in private locations, and not public locations. Users will be trained to recognized likely eavesdroppers who may be hacking, sniffing, or setting up malicious code.
18. Laptop and **[insert type of device(s)-for example, “Smartphone and Tablet”]** users are not allowed to change any setting or security rule on their laptops or **[insert type of device(s)-for example, “Smartphone and Tablet”]** without permission from the Security Official.
19. Laptop and **[insert type of device(s)-for example, “Smartphone and Tablet”]** users must adhere to the general **[organization]** computer and internet use policy including not downloading software, introducing foreign media, and so forth.
20. Laptops and **[insert type of device(s)-for example, “Smartphone and Tablet”],** when in transit, must be carried in the user’s immediate vicinity with appropriate covers or containers. Laptops and **[insert type of device(s)-for example, “Smartphone and Tablet”]** should not be left unattended.
21. Laptops and **[insert type of device(s)-for example, “Smartphone and Tablet”]** when in use at the employee/contractor’s home should be used in a secure location and only by the employee/contractor and not by family/friends or other unauthorized individuals. Users may not use their devices or remotely access ePHI in the immediate presence of any unauthorized person, family or friend who might view the information.
22. Flash drives and other media copying of ePHI will only be used if password protection is enabled and the drive or media is encrypted and provided by the Security Official.
23. All remote access to the **[organization]** networks or cloud-based applications with ePHI shall be done with the use of a secure access **[insert the type of access; for example if you have set up a VPN]**.

I have read this policy and procedure and will adhere to its requirements:

­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Employee/Contractor Date