|  |  |
| --- | --- |
| **Company Name or Logo1**  **Policy and Procedure** | |
| **Title: Mobile Phones** | **P&P #:**  IS-1.8c |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology (TVS012)** |

**Mobile Phones**

**Definitions**

Mobile Phones – Any portable phone device (smart or otherwise) that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing confidential information. Examples of mobile phones may include, but are not limited to: cell phones, smartphones, etc.

Confidential Information – Any individual’s Protected Health Information (PHI) as defined by HIPAA; financial, operating or other proprietary of the Practice; and other information of the Practice that is confidential in nature (i.e., employee compensation, benefit and disciplinary records).

**Mobile Phone Usage Standards and Policy**

Only Practice owned mobile phones are permitted for conducting Practice business requiring the use of a mobile phone. The use of a personal mobile phone for conducting Practice business is strictly prohibited unless the use of a personal mobile phone has been approved by an employee’s department head and the Practice Security Officer.

Approval Procedure **–** For permission to activate and use a Practice mobile phone you will be required to receive the approval of your immediate supervisor or department head and the Security Officer or other appropriate personnel of the Practice. Use the Network Access Request Form to make this request. If the use of a personal mobile phone has been approved for an employee, the employee must also agree to and sign the Bring Your Own Device Agreement (located in Appendix I). Once this form is completed and approved you will be contacted by appropriate Practice personnel to setup your mobile device and schedule training.

General Requirements – All of the Practice’s standard computer equipment security requirements are in effect for mobile phones as well. These requirements include, but are not limited to:

* Strong authentication using password, PIN and/or biometric security
* Prohibition of installing unauthorized software
* Prohibition of modifying configuration settings

Other Requirements – The portable nature of mobile phones requires procedures which may not be applicable for workstations or similar computer equipment. Your mobile phone training will include these mobile phone specific requirements. These requirements include, but are not limited to:

* Your duty to report a lost or stolen mobile phone to the Practice Security Officer immediately.
* Receiving approval from your supervisor prior to working on your mobile phone after hours or after the number of hours for an applicable work period has been reached.
* Your mobile phone must be kept in a secure location when not in use and never left unattended.
* Unless specifically authorized by Practice management, recording any video, still pictures or audio with a mobile phone is strictly prohibited.

Software Requirements **-** The following is a list of minimum operating system versions for various mobile phones required for conducting Practice business on mobile phones:

{list supported mobile phones here}

If your mobile phone does not meet this minimum requirement, please notify your supervisor or department head so that the mobile phone can be updated.

Training Requirements **-** Once you have approval for the use of your Practice mobile phone, you will be required to attend a mobile phones usage and security training session provided by the Security Officer or other appropriate personnel. This training session will cover the secure use of your mobile phone. This training will be conducted within a reasonable period of time once mobile phone usage has been approved, and in most cases will include several individuals at once.

End of Use - When no longer in productive use, all mobile phones must be wiped of data in a manner which conforms to HIPAA regulations. To ensure proper reuse and disposal procedures are followed, all mobile phones must be returned to the Security Officer or other appropriate personnel for data erasure when no longer in use.

Employee/Contractor Termination - When an employee or contractor leaves the Practice, any mobile phones in their possession must be returned to the Security Officer or other appropriate personnel by the employee’s or contractor’s supervisor or department head for data sanitization conforming to HIPAA guidelines for the reuse or disposal of electronic equipment.