**Security Policy #9**

**Bring Your Own Device (BYOD) Policy**

**Purpose of Policy**

The purpose of the policy is to develop the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices. Proper security controls are essential to protect any sensitive information that may be on these devices. Documented instructions and requirements should be provided to all employees that may be accessing or storing PII and sensitive company data on their personally owned devices and acknowledgement of acceptance should be documented and retained.

**Bring Your Own Device (BYOD) Policy**

1. The Company may be responsible for any breaches of PII and may suffer consequences of breached sensitive company data that resulted from unsecured employee personally owned devices.
2. Employees must be aware that breaches or inappropriate use of their devices that may put PII and/or sensitive company data at risk may negatively affect customers, The Company and the employee themselves. The Company has the right to revoke an employee’s access to PII and/or sensitive company data or levy sanctions laid forth in The Company’s sanction policy.
3. Encryption of devices usually offers a safe harbor under federal and state regulations and is the strongest protection against a data breach. Encryption should be used on all devices that access or store PII and/or sensitive company data.
4. Employees are not permitted to access PII and/or sensitive company data, on personally owned devices, unless authorized and approved.  Only approved devices that are properly configured will be given access to PII and/or sensitive company data.
5. The Company will limit who has access to PII and/or sensitive company data on their personally owned devices. The Company will provide employees with only the limited amount of access to PII and/or sensitive company data to perform their job function.
6. The organization and their Information Technology (IT) group/provider will work together to manage and enforce this Bring Your Own Device (BYOD) policy.

**Procedure**

1. The Company will communicate this policy to their employees. Employees must request permission to use personally owned devices and fill in the registration form provided.
2. The Company and IT will periodically review and update this policy when new requirements are implemented or when security requirements change. Employees must be notified of any changes and a document of their acceptance/acknowledgment should be collected.
3. The Company and IT reserve the right to monitor and inspect devices registered in its BYOD program to ensure that PII and sensitive company data are being properly protected.
4. Upon an employee’s termination of employment, The Company and IT will ensure that any devices the employee has with PII and/or sensitive company data are returned to IT for a final analysis and removal of any PII and/or sensitive company data or applications that access PII and/or sensitive company data. This will be conducted as soon as possible to limit inappropriate access to PII and/or sensitive company data.
5. Documentation, acknowledgement and registration forms will be retained for all employees and kept in their employee folder. Documentation must also be provided to employees initially and upon request.

**Appendix A**

**Bring Your Own Device Policy**

This document provides the guidelines for a Bring Your Own Device (BYOD) policy for The Company. It offers principles to help guide employees and staff and can be modified by the company to better reflect their specific needs.

The Company’s employees have the ability to bring and utilize various personal devices that may have the ability to access, store or transmit PII and/or sensitive company data. Devices include but are not limited to smartphones, tablets and laptops. Employees must be aware that when accessing PII and/or sensitive company data on their personally owned devices, they must protect that information. The ability for employees to utilize personally owned devices at the office should be treated as a privilege and The Company reserves the rights to revoke this privilege if an employee does not abide by the policies laid forth.

**Devices Permitted**

Smartphones accepted (brand and model): ­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tablets accepted (brand and model): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Laptops: personally owned laptops must be accepted and approved by (company name) management.

Additional Devices: other additional personal devices that may access or store patient information must be approved by (company name) management and IT.

Specifically excluded devices: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Security Specifications**

Mobile Device Management service:

Encryption service:

Anti-Malware/Anti-Virus service:

Minimum Operating System required (laptop):

Minimum Operating System required (smartphones):

Minimum Operating System required (tablets):

Secure texting application required:

System Inactivity timeout setting (minutes):

Email Encryption provider:

**Security Requirements**

* All devices must be password protected.
* Passwords must be complex; requiring a minimum of 6 characters, a combination of upper- and lower-case letters, numbers and symbols.
* Devices must lock after five incorrect password attempts.
* Devices must “time out” and require a password after a five minute period of inactivity.
* Text messages that may contain PII and/or sensitive company data must be sent through the secure texting application provided. **If a secure texting application has not been provided then employees should not send PII and/or sensitive company data via text.**
* Emails that are sent through the device containing PII and/or sensitive company data must be sent encrypted. **If secure email encryption is not provided, employees should not send email that contain PII and/or sensitive company data via email.**

**Restrictions and Limitations**

* “Rooted” or “Jailbroken” devices are not permitted to access PII and/or sensitive company data.
* Employees must notify management when selling, trading in, recycling or disposing of their personal devices.
* The employee’s device may have data remotely deleted / wiped if 1) the device is lost or stolen, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of The Company’s data and/or technology infrastructure.
* Devices that are lost or stolen must be reported to management and/or IT as soon as possible but within 24 hours.
* Employees must inform management and/or IT if they plan to upgrade, recycle or dispose of their personally owned device.
* Employees who voluntarily resign from the organization must present their device(s) to management and/or IT within 48 hours to have all PII and/or sensitive company data and/or access deleted / removed from the device.
  + Employees who do not turn over their device(s) to management and/or IT within 48 hours after voluntary resignation are subject to a full remote wipe / deletion of all data including non PII and sensitive company data on their device.
* The organization will prepare for scheduled terminations in advance and ensure that employees present their device(s) to management and/or IT the day of the scheduled termination to have all PII and sensitive company data and/or access deleted / removed from the device. Terminated employees that do not present their device(s) will be given an opportunity to bring in their device(s) to have all PII and sensitive company data removed from the device(s). Terminated employees that fail to bring in their device(s), after given the opportunity, are subject to a full remote wipe / deletion of all data including non PII and/or sensitive company data on their device.

**Additional Information**

The organization will provide any additional specifications, requirements or restrictions in this section.

**Sanctions**

Violations or abuse of this policy are subject to the repercussions laid out in The Company’s sanction policy.

**Bring Your Own Device – Device Registration form**

Employee name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position/title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Secondary Phone number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Device and Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Serial Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ MAC Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Access points; where will patient information be accessed (email, text messages, applications, web etc.):

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

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

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

Device Security Specifications (for IT and/or (company name) management to complete):

|  |  |  |
| --- | --- | --- |
| **Security Specification** | **Implemented (yes or no)** | **Details or additional information** |
| Operating system |  |  |
| Encryption |  |  |
| Anti-virus service |  |  |
| Secure Texting Application |  |  |
| Timeout/lock settings |  |  |
| Password requirements |  |  |
| Web browser |  |  |
| Mobile wipe |  |  |
| E-mail provider |  |  |
|  |  |  |

Additional information, specific device restrictions and requirements should be detailed below:

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

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

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

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

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of personally owned devices that may access, store or transmit PII and sensitive company data. I am aware that violations of this guideline of appropriate use may subject me to retraction of this privilege or disciplinary action, including termination of employment. I further understand that inappropriate use of my device that may put PII and sensitive company data at risk may negatively affect customers, The Company and myself.

I am aware of the technical restrictions and requirements on my device that were provided in the device registration form. I will maintain and manage these security requirements on my device for as long as I continue to access, store or transmit PII and sensitive company data. I understand that The Company reserves the right to protect their customer’s information as well as sensitive company data that I may be accessing and therefore have the ability to remotely wipe / delete data from my device if the need arises.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature | Date |

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Requestor’s Immediate Supervisor Signature | Date |

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Information Technology Provider’s Signature | Date |