Compliancy Group

Sample BYOD Policy

HIPAA SEAL OF COMPLIANCE COMPLIANCY GROUP

HIPAA VERIFIED

Introduction

This document provides policies, standards, and rules of behavior for the use of personally-owned devices (Laptops, smartphones and/or tablets) by (Insert your Organization Name) employees to access the Organization's resources and/or services. Access to and continued use of resources and/or services is granted on condition that each user reads, signs, and abides by the Organization's policies concerning the use of these resources and/or services.

Purpose of Policy:

This policy is intended to protect the security and integrity of an Organization's data and technology infrastructure. Limited exceptions to the policy may be granted because of variations in devices and platforms.

This BYOD policy discusses parts of a HIPAA compliance program. This policy does not make your business HIPAA compliant. If you would like more information on how to become HIPAA compliant please visit www.compliancy-group.com/why-cg/ or give us a call at 855-854-4722.

Expectation of Privacy: The Organization will respect the privacy of your personal device(s), and will only request access to the device:

- When needed by IT personnel to implement security controls; or
- To respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

Please Note: *This sample BYOD Policy differs from the policy(ies) governing use of Organization-provided equipment and/or services. With respect to such equipment and/or services, employees neither have a right of privacy nor an expectation of privacy, with respect to the use of equipment and/or services.*

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the Organization's business.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game- playing.
- Personally-owned Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information
  - Harass others
  - Engage in outside business activities
- Employees may use their personally-owned devices to access the following company-owned resources:
  - Email, Calendars, Contacts, Documents
- The Organization has a zero-tolerance policy for texting or emailing while driving. Only hands-free talking while driving is permitted.

Devices and Support

- The following devices are supported:
  - iPhone, iPad, Android, Blackberry, Windows, Mac
- Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for an operating system or hardware-related issue.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software, and security tools, before they can access the network.

Security

- In order to prevent unauthorized access, devices must be password-protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- All devices must be encrypted according to NIST guidelines
- The device must lock itself with a password or PIN if the device is idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Laptops, Smartphones, and tablets that are not on the company's list of supported devices are not allowed to connect to the network.
- Laptops, Smartphones, and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if:
  - The device is lost or stolen.
  - The employee terminates his or her employment.
  - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The Organization reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of (Organization Name) services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided. By attesting that I, the named employee, understand this policy, that I will abide by its business practices and if not will face disciplinary actions.

Signed and Agreed to by:

Employee Signature: _____ Date: _____

Print Name: _____ Title: _____

Supervisor Signature: _____ Date: _____

Print Name: _____ Title: _____