AKDHC NKDHC Nevada Kidney Disease & Hypertension Centers PKDHC Pediatric Kidney Disease & Hypertension Centers

BYOD Policy	Created: 10/26/2016
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 7

AKDHC, NKDHC & PKDHC is hereinafter referred to as "the company."

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security and use of mobile devices.

2.0 Purpose

The purpose of this policy is to specify company standards for the use and security of mobile devices.

3.0 Scope

This policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. **Since the policy covers the data itself, ownership of the mobile device is irrelevant so that any and all devices that come in contact with company data are subject to monitoring such that employees should have no reasonable expectation of privacy. This policy covers any mobile device capable of coming into contact with company data.**

4.0 Policy

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The company considers the physical security of its mobile devices and employees will take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.

- Mobile devices will be configured to auto lock with a passcode within 1 minute and should be kept out of sight when not in use.

- Care should be given when using or transporting mobile devices in busy areas.

- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

- The company has determined the data that will be stored on mobile devices is considered confidential and in the event of loss remote wipe/remote delete is mandatory. This technology allows a user or administrator to make the data on the mobile device unrecoverable and should be considered by the employee. It is considered the employee’s responsibility to ensure proper backup procedures are taken in accordance with the Prime Backup Policy.

- The company will continue to monitor the market for security products for mobile devices, as it is constantly evolving.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting company data. The following sections specify the company's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

Whole Disk or Encryption (Physical or Logical Disk) using Software or Hardware is encouraged and required when working with electronic Patient Health Information (ePHI) and/or if data stored on the device is especially sensitive. Laptops require an approved username and password and/or biometrics for login.

4.2.2 PDAs/Smart Phones

Use of encryption is not required on PDAs/smart phones but it encouraged if data stored on the device is especially sensitive. PDAs/smart phones must require a password for login.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of company data on such devices is strongly discouraged, but their use is permitted and encryption is not required.

4.2.4 Portable Media Players

No company data can be stored on personal media players.

4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the company.

4.4 Corporate Account Access and Billing

4.4.1 Corporate Account Access

4.4.2 Reimbursement for Accessories / Software

4.4.3 Data Usage

While sending texts or e-mails, or browsing the Web for work-related reasons via mobile devices is accepted, employees should keep in mind that this usage is billed with a maximum limit and over usage costs may vary and are billable to the company. The amount of data usage is checked at the end of each billing cycle, employees are responsible for maintaining within acceptable data usage limits. Access to non-approved applications, email accounts and personal information via mobile devices which incur additional charges are that there will be consequences for abusing

4.4.4 Mobile Device Upgrades

4.4.5 Mobile Device Repair

4.5 General Guidelines

The following guidelines apply to the use of mobile devices:

- Company-provided mobile devices are to be used for business purposes only. Misuse is cause for termination.

- Loss, Theft, or other security incident related to a company-provided mobile device must be reported promptly.

- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.

- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

- Social Media use on company provided phones….

- Personal Calls to be taken outside of work environment to avoid disturbing others.

- Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

4.5.1 General Cell Phone Etiquette

- *No phone use during meetings.* Employees to step out to take calls or send texts when business meetings, conferences, or brainstorming sessions are being held. Use of the vibrate function

- *The 'vibrate' function is your best friend.* When working in a professional atmosphere, the vibrate function should be a default. No one likes a loud ringer – especially when left unanswered.

- *Letting calls go to voicemail isn't a sin.* According to a survey of 1,500 adults by the Pew Research Center, 24 percent of them said they felt obligated to take a call – even if it interrupted an important meeting. Voicemail, however, can be just as efficient in communicating with others outside of work.

- *Maintain low tones*. There are few things more annoying than a loud phone conversation, and that rings doubly true when people are trying to get work done. Clearly explain to employees to keep a low voice if they must answer their cell phones, or find a quiet area to talk. It might also be helpful to designate a specific area, like a lobby or cafeteria.

- *Content and language guidelines*. It's not uncommon for a customer to be offended or even turned away as a result of an employee's expletive-filled phone conversation. Professional communication is not the same as communication at home, and your policy should delineate the difference.

4.3 Mobile Device Camera Use

The use or presence of mobile camera phones in the workplace may interfere with productivity and lead to problems, including personal conflicts, privacy violations, and the unauthorized disclosure of confidential information. In an effort to reduce the risk of a deliberate or accidental use of images for inappropriate purposes employees are to avoid any impropriety or harassment associated with the use of mobile camera phones. This is especially true in places where employees and visitors have an expectation of privacy, such as bathrooms, locker rooms, dressing areas, etc.

For example, The State of Texas is very strict when it comes to the violation of a person's privacy. Producing a non-consensual image of another person can lead to a felony charge, which may result in jail time or steep fines. Considering the number of devices that have cameras, this response is used as a deterrent against would-be peeping toms.

If caught filming or photographing a person in these areas without his or her consent, the law may bring harsh punishment against the offender. In addition, the punishments for this crime may increase if the person being photographed is a minor.

Mobile Device Cameras are to be used for business purposes only and are subject to monitoring such that employees should have no reasonable expectation of privacy for pictures or videos for all devices capable of coming into contact with company data.

- Employees will be disciplined on a case-by-case basis and appropriate remedies taken, up to and including termination, for violating the policy.

4.3 Mobile Device Use while Driving

Company provided mobile devices are not to be used while driving. If you must make a call, read an email or use your mobile device, pull off the road to do so. Employees that violate the policy and become involved in an accident must assume full liability for damages. Employees who are involved in accidents or who violate state laws concerning the use of mobile devices may be subject to disciplinary action up to and including termination.

4.3 Mobile Device Use in High Hazard Zone

4.6 Audits

The company will conduct periodic reviews to ensure policy compliance. A sampling of mobile devices will be taken and audited against this policy on a periodic basis.

4.7 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices A portable device that can be used for certain applications and data storage. Examples are PDAs, Tablets, Laptops or Smartphones.

Mobile Storage Media A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

7.0 Revision History

Revision 1.0, 10/26/2015