	Guideline: ITS Personal Device Use Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Entire workforce

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), confidential, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure defines roles, responsibilities, and processes associated with the use of personally owned devices in the workplace.

Scope and Goals:
This procedure applies to all personally owned devices used in the workplace. Personally owned devices are defined as smartphones, laptops, tablets, electronic media, etc. (hereafter referred to as personal devices).

The goals of this procedure are as follows:

- Ensure workforce members understand their responsibilities for safeguarding covered information when using personal devices to access Cone Health technology resources.
- Ensure workforce members understand what is considered acceptable behavior when using their personal device for work.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to, the following activities:

- Revision, implementation, workforce education, interpretation, and enforcement of this procedure.
- Assist ITS with the implementation of mobile device management technology.
- Providing training to personnel on the use of personal devices in the workplace, to include providing these workforce members with a list of approved applications, application stores, and application extensions and plugins.
- In coordination with the workforce member's supervisor, approve the use of personal devices for work.
- Revocation of personal device use privileges, when it is determined that a workforce member is not compliant with this procedure.

Guideline: ITS Personal Device Use Procedure

Information and Technology Services (ITS):
ITS is responsible for implementing mobile application management technology that enforces security controls on applications for personal devices when they connect to Cone Health technology resources.

Management:
Individual department managers are responsible for evaluating the business need of each workforce member under their supervision as to whether their use of a personal device for work is justified.

Workforce:
Workforce members approved to use their personal devices for work are responsible for the following:

- Abiding by the requirements set forth in this procedure.
- Immediately informing the CISO and ITS of a lost or stolen personal device.

Acceptable Use:
Acceptable use is defined as activities that directly or indirectly support the business. In addition to what is covered under Cone Health's Email and Internet Acceptable Use agreements and Cone Health's Access Terms and Conditions Agreement, the acceptable use rules apply to the use of personal devices for work:

- Cone Health defines acceptable personal use during business hours as "reasonable and limited" personal communication with family and friends, leisurely reading, and game playing.
- At the discretion of the organization, workforce members will be blocked from accessing certain websites during work hours/while connected to the organization's network. For those instances where an inappropriate site (as defined by the Internet Acceptable Use Agreement) is not blocked, workforce members will use professional ethical judgment not to access them.
- Personally owned devices' camera and/or video capabilities are not authorized to be used in the workplace.
- Personally owned devices will not be used at any time to:
    - Store or transmit illicit or illegal materials
    - Harass others
    - Engage in private business activities (outside normal business hours is okay)
- Transmission of covered information over the internet, public carrier lines, and Wi-Fi must be encrypted.
- Workforce members will maintain proper physical control of their personally owned device at all to times and will not share their device with any other person to include family members if it contains or is suspected to contain covered information or is connected to Cone Health's network.
- Personally owned removable media will not be used on Cone Health's network or with any related information systems.
- Personally owned devices will be allowed to store or transmit covered information by approved Cone Health applications
- Approved Cone Health applications must ensure that data is either not stored locally on the device or stored in an encrypted container that is accessible only from other protected applications. Also, the application must utilize a security password or PIN and automatic lockout screen setting in place to prevent unauthorized access.

- The following applications are allowed on personally owned devices used in the workplace: Outlook Mobile, Microsoft Authenticator, OneDrive, Microsoft Teams, Microsoft PowerApps, Microsoft Word/Excel/PowerPoint/Visio, Citrix Workspace, Cisco WebEx, Cisco Jabber, ServiceNow Mobile, UKG Workforce/Kronos Mobile, Epic MyChart, Epic Haiku, Epic Canto
- Applications not on the allowed list will be approved by the CISO prior to interacting with Cone Health systems or data.
- Applications purchased by the workforce member that are used for work related purposes will be considered the property of Cone Health.
- Workforce members will forfeit their device without question to Cone Health if the device is determined to be involved in a security/privacy related investigation, incident, breach, or criminal or civil litigation.
- Employees may use their personally owned devices to access the following company-owned resources: email, calendars, contacts, documents, teams, Citrix applications, ServiceNow, WebEx, UKG Workforce/Kronos, and Epic
- Cone Health has a zero-tolerance policy for texting or emailing while driving. Only hands-free talking while operating a motor vehicle is permitted.

Security Requirements:

To ensure covered information and access to Cone Health resources are protected against confidentiality, integrity, and availability risks, approved applications must have the following security features enabled or they will not be allowed to be used for work related purposes or access Cone Health resources:

- Application must use password/passcode protection. Four-character passcodes will be used that are not easily guessed. Passcodes will be random, non-sequential, and comprised of four different numerals. Fingerprint and facial recognition are acceptable as long as a passcode is also used as a backup.
- Application must be configured to lock after 60 minutes of inactivity.
- Application will be configured to auto-erase their contents and convert back to factory settings after 5 failed passcode entry attempts.
- Personally owned devices will have Bluetooth turned off until needed and then turned back off when no longer needed.
- Personal hotspot will be turned off until needed and then turned back off when no longer needed.
- Rooted (Android) or jail-broken (iOS) devices are strictly forbidden from accessing the application.
- Application must ensure that it is kept up to date with the current security patches (i.e. version).
- Workforce members will have limited access to Cone Health data based on defined Cone Health user roles.
- Workforce members consent to having their device activity monitored and grant Cone Health ITS the authority to remotely wiped (erase) Cone Health data from their device if 1) the device is lost or stolen, 2) the employee terminates his or her employment, 3) Cone Health detects a data or policy breach, a virus or similar threat to the security of covered information or the organization's technology infrastructure.

- Before turning in a personal device to a vendor for upgrade, replacement, etc., the workforce member will ensure all covered information has been removed from the device and all connectivity Cone Health resources has been terminated. Ideally, the member will revert the device back to its factory setting.
- Cone Health applications must ensure that data is either not stored locally on the device or stored in an encrypted container that is accessible only from other protected applications.

Personally Owned Devices and Support:
Cone Health ITS support of personally owned devices is limited to the Cone Health approved application list. Workforce members will contact the device manufacturer or their service carrier for operating system, hardware-related or performance issues.

Risks/Liabilities/Disclaimers:
While Cone Health will take every precaution to prevent a workforce member's personal data from being impacted, it is the member's responsibility to take additional precautions, such as backing up contacts, etc. All Cone Health covered information stored on the device, to include post-termination of employment/contract (voluntary or involuntary) will be governed by Access Terms and Conditions Agreement and Cone Health's privacy policies. Workforce members also understand that:

- The company reserves the right to disconnect devices or disable application services without notification.
- Lost or stolen devices must be reported to the CISO and ITS within 24 hours. Members are responsible for notifying their mobile carrier immediately upon loss of a device.
- Workforce members are expected to use personal devices in an ethical manner at all times and adhere to the organization's acceptable use policies.
- Workforce members are personally liable for all costs associated with his or her device.
- Workforce members assume full liability for risks including, but not limited to, the partial or complete loss of organizational 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.
- Cone Health reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this procedure.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are directly compensated for services/work by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by

requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.