Medicine
Information Services

# Smart Device Policy

**General Policy**

- Individuals with CU Medicine email addresses may synchronize their personal Smart Device with CU Medicine's email system with management approval.

- Non-exempt employees may not synchronize their CU Medicine email to a personal Smart Device. Any exception to this policy must be reviewed by Human Resources.

- CU Medicine's email system is intended for business use. Therefore, use of the CU Medicine email system for commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations is prohibited.

- Because the Smart Device is being used for business purposes, corporate email and/or documents thereon are the property of CU Medicine. CU Medicine may monitor employee computer files and software. CU Medicine maintains the ability to access and monitor CU Medicine messages and attachments transmitted over the CU Medicine email system. CU Medicine management or a designated representative may access or monitor CU Medicine messages or attachments transmitted using the Smart Devices. Additionally, the Smart Device may need to be included in a forensic investigation.

- Upon termination of employment, all email and email attachments must be removed from an employee's personal Smart Device by the CU Medicine Information Services (IS) Department.

- In accordance with CU Medicine's security policies, user account identifiers, personal access codes and passwords are not to be shared with others.

- Due to the periodic changes of security standards, CU Medicine's Smart Device policies may change at any time.

**System Policies**

- All Smart Devices connected to the CU Medicine Exchange Server will have a CU Medicine IS security policy applied. The policy will:

    - Require a security lock with a minimum of 5 characters.
    - Prohibit security lock from being disabled.
    - Prohibit reuse of passwords for an extended period of time.
    - Turn on screensaver/key lock after 30 minutes of idle time.
    - Force the device to lock and wipe after 10 failed attempts of typing the password/passcode.
    - Enforce password expiration every 180 days.

**Security Guidelines**

- Lock the device by turning on the key lock when not in use.

- Diligently protect the device from loss and from disclosure of private information belonging to or maintained by CU Medicine or its affiliate networks. **Contact the CU Medicine Helpdesk at 303-493-8000 immediately to report any lost or stolen device.**

- Sensitive and private corporate information such as social security numbers and protected health information should not be stored on Smart Devices. To protect against inadvertent disclosure, only store absolutely necessary information on the device.

- All CU Medicine Outlook data (email, contacts, calendar, etc.) is backed up on CU Medicine servers according to CU Medicine's standard back-up schedule. Outlook mailbox data including contacts, calendar items, email and email attachments are encrypted. This data may be viewed on the device, but no other corporate documents are to be stored on the device.

- CU Medicine reserves the right to audit any device connected to its network.

- Understand that conversations spoken over a hands-free headset are NOT confidential as these conversations can be inadvertently or intentionally intercepted within 100 meters on some Bluetooth device.

- Corporate passwords should not be stored on a Smart Device nor should safe/door combinations, personal identification numbers or confidential, private, sensitive, or proprietary information.

- A Smart Device is considered to be a portable workstation and all CU Medicine security policies apply. CU Medicine's security policies are available on the corporate intranet at https://intranet.cumedicine.us/documents-resources/policies/

| Version | Date | Revision Notes |
|---|---|---|
| A | 5-19-2017 | Policy updated |