Information Security Workforce Summary

Information privacy and security are prevalent issues in the government, healthcare, public, and private business sectors. Many federal and state regulatory laws have been enacted, and industry leaders in finance, such as VISA and MasterCard, are enforcing ongoing measures to improve the security of individuals' data and the protection of privacy.

In accordance with these requirements, it is necessary for University of Colorado Medicine (CU Medicine) to maintain the security of the information that is stored, transmitted, and processed within the organization. Security policies are in place as part of CU Medicine's program to address information security.

This document is intended to provide a practical overview of CU Medicine's security policies as they apply to "workforce members," a term applied to all individuals engaged in work for CU Medicine including but not limited to employees, outside contractors, and temporary workers through outside agencies. To access these policies in their complete form, as well as the other instructions and forms referenced in this document, please visit the CU Medicine corporate intranet website at http://intranet.cumedicine.us/departments/information-services/.

These policies apply to all CU Medicine Administrative and CU Medicine Cost Center workforce members at all locations.

For questions or more information, please contact the CU Medicine Help Desk (303-493-8000) or send an email to helpdesk@cumedicine.us.

University of Colorado Medicine
Information Security Workforce Summary

Workforce Security

- Workforce members must understand and comply with all CU Medicine information security policies and procedures. Those using affiliate systems may need to comply with additional policies and should contact the appropriate organization for instruction.

    - University of Colorado Denver (UCD), Regulatory Compliance 303-724-1010
    - University of Colorado Health (UCH), Help Desk 720-848-4000
    - Children's Hospital Colorado (Children's), Help Desk 720-777-4357

- The CU Medicine Information Services (IS) Department performs internal security audits as described in its "Computer Security Audit Policy".

- CU Medicine maintains a policy and process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.

- All individuals who access CU Medicine information systems must sign the "User Account Security Acknowledgement Form" affirming their responsibility for the protection of the confidentiality, integrity, and availability of CU Medicine information systems and processes.

- Workforce members are responsible for appropriately safeguarding electronic protected health information (ePHI), credit/debit card, and other private/sensitive information from unauthorized access, modification, destruction, and disclosure. Information that must be protected includes but is not limited to:

    - Patient records that contain names, dates of birth, medical record numbers (MRNs), addresses, telephone numbers, dates of service, diagnoses, procedures, and other specific medical information.
    - Social Security numbers.
    - Credit card information.
    - Bank account information.
    - Employee/personnel records including driver license numbers, background investigation information, birthdays, and other personal information.

- As stated on the "User Account Security Acknowledgement Form", all activities on CU Medicine's information systems may be monitored and recorded. Individuals using CU Medicine information systems expressly consent to such monitoring.

- Workforce members must not attempt to gain access to information systems containing sensitive information for which they have not been given proper authorization.

- Workforce members must not provide unauthorized individuals access to any information systems containing ePHI or any other sensitive information. This includes not providing access even to other workforce members who are authorized access to the data.

University of Colorado Medicine
Information Security Workforce Summary

- Prior to employment, internal transfer, or promotion, CU Medicine may perform an employee background check.

- When workforce members terminate employment from CU Medicine, physical and information systems access is revoked. All CU Medicine supplied equipment must be returned by the time of departure. Equipment includes but is not limited to:

    - Desktop and laptop computers.
    - Building, desk, and office keys.
    - Access cards.
    - Other assigned property and equipment.

Security Awareness Training

- Workforce members must receive security training. Security training is delivered as a component of CU Medicine's New Employee Orientation. Additionally, all Administrative employees must attend the Computer Orientation class. The manual for this class is available on CU Medicine's corporate intranet website.

- Security reminders are sent out on a periodic basis and also are available on CU Medicines corporate intranet website.

Security Incidents

- A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or unauthorized interference with computer system operations. The incident could be either accidental or intentional and caused by internal or external activities or events.

- Workforce members must report an observed or suspected security incident as quickly as possible to the CU Medicine Help Desk (303-493-8000) and provide the following:

    - Incident description.
    - Date and time of incident.

- Examples of security incidents include but are not limited to:

    - Password sharing.
    - Lost or stolen computer device or electronic media.
    - Unauthorized access to ePHI, PCI, or other sensitive data.
    - Illegal or unethical activities, such as cyberstalking, harassment, and pornography.
    - CU Medicine premises break-in.
    - Infections by malicious code, such as viruses and worms.

University of Colorado Medicine
Information Security Workforce Summary

- A UPI workforce member must not prevent another workforce member from reporting a security incident.

Physical Security

- All visitors (except Member Faculty) to the CU Medicine Administrative Building must:
    - Sign in at the designated reception desk.
    - Show proper identification and state reason/person they are visiting.
    - Wear a visitor badge and be escorted while on-site, particularly in areas where information systems containing sensitive/restricted data are maintained (UCD, UCH, and Children's affiliates do not need to wear a visitor badge if they are wearing their organization's ID badge).
    - Remove the badge when signing out at the front desk and leaving the site.

- The reception area and patient interview rooms located on the 6th floor of the CU Medicine Administrative Building are considered public areas and do not require a visitor badge.

- Workforce members must not attempt to gain access to CU Medicine restricted facility areas and information systems without proper authorization. Restricted areas include but are not limited to:
    - Telecommunications closets.
    - IS Department work area.
    - Data centers.

- Workforce members must immediately report to appropriate management the loss or theft of any device (e.g., key, card, or token) that enables them to gain physical access to CU Medicine facilities.

Workstation Use/Security

- CU Medicine workstations are intended for business use. Such use shall demonstrate respect for intellectual property, ownership of data, and security controls. Workstations include but are not limited to desktops, laptops, and smartphones.

- Workforce members must not use CU Medicine workstations or any other computer equipment to engage in any activity that either is illegal under local, state, federal, or international law or is a violation of CU Medicine policy.

- Workforce members must not use CU Medicine workstations or any other computer equipment to:
    - Violate the privacy of patients, employees, or providers.
    - Install or distribute “pirated” or other unlicensed software products.
    - Deliberately introduce malicious software onto a workstation or network (e.g., viruses and spyware).

  - Purposefully cause security breaches. Security breaches include but are not limited to accessing electronic data or logging into an account that the workforce member is not authorized to access.
  - Engage in any form of unauthorized network monitoring that will intercept electronic data not intended for the workforce member.
  - Circumvent or attempt to avoid the user authentication or security of any CU Medicine workstation or account.
  - Transmit, store, or access material which has the purpose or effect of creating an intimidating, hostile, or offensive work environment.
  - Threaten, harass, or stalk another individual or group.

- Any workstation used by a CU Medicine workforce member for business purposes should be secured by using an initial login and password.

- Laptop computers and smartphones should be configured with the power-on password enabled.

- All software installed on CU Medicine owned and supported workstations is to be installed by CU Medicine Information Services (IS) staff as described in the "Computer Software Installation and Support Policy".

- Screensavers with password protection should be enabled on any workstation used by a CU Medicine workforce member for business purposes.

- Workforce members should activate their workstation lock whenever they leave their workstation unattended.

- Workforce members must log off from or shut down their workstation(s) when their shifts are completed.

- Workforce members must take reasonable measures to prevent viewing of sensitive data on workstations by unauthorized persons. This includes preventing viewing even by those CU Medicine and affiliate workforce members who might not have authorization to view a particular data.

- Unauthorized CU Medicine workforce members must not attempt to gain physical access to workstations that can access sensitive information.

- Any workstation used for business purposes transported and/or used off-site must be securely maintained. Workstations must be handled as carry-on baggage when on public transport. They must be concealed and/or locked when in private transport.

- All UPI owned and supported computer hardware is to be installed and/or connected to the network by CU Medicine IS staff as described in the "Computer Hardware Installation and Support Policy".

University of Colorado Medicine
Information Security Workforce Summary

Media Protection

- Information systems and electronic media include but are not limited to:

    - Workstations such as desktops, laptops, and smartphones.
    - Servers.
    - Floppy disks and CD-ROMs.
    - Zip drives and portable hard drives.
    - USB portable storage devices such as thumb drives, memory cards, and MP3 devices.

- All CU Medicine information systems and electronic media containing sensitive information must be properly disposed of when no longer needed. Portable electronic media is to be disposed in the recycling bin located in the IS Department.

- All sensitive information on CU Medicine information systems and electronic media must be removed before such media can be re-used. However, if portable media is to be shared with another individual, use new media. Portable media should be written over only for an individual's own re-use. Credit card information, ePHI, and other personally identifiable or sensitive information should not be stored on any employee-owned media or device.

- Information systems and electronic media are not to be removed from CU Medicine's premises without management permission. Employees provided with laptops to use as their primary computer are exempt from this prohibition.

- All movement of CU Medicine information systems and electronic media containing ePHI or other sensitive information into and out of CU Medicine facilities must be tracked and logged. Those responsible for using portable media such as laptops and other removable storage devices must take all appropriate and reasonable actions to protect the information contained on the device.

- Sensitive information should not be stored on workstations or portable electronic media. It is strongly recommended that all sensitive information be saved to network drives where the data can be backed up.

- Workforce members must immediately report the loss or theft of any information system or electronic media to the CU Medicine Help Desk (303-493-8000).

- Printed media containing sensitive information must always be protected.

University of Colorado Medicine
Information Security Workforce Summary

Authentication Protection

- Workforce members must have and use their own assigned unique identifier or username to access UPI information systems.

- Workforce members must not share or reveal their authentications (e.g., passwords and PINs) with others. Sharing an authentication can make the authorized user responsible for actions that another party takes with the disclosed information. Passwords should be complex and protected as described in the "Security Password Policy".

- All activities on UPI information systems may be monitored and recorded. Individuals using CU Medicine's information systems expressly consent to such monitoring.

- Inappropriately used, lost, or stolen authentications must immediately be reported to the workforce member's manager and the Information Services Department.

Security of Transmitted Information

- All sensitive data transmitted outside of the CU Medicine and Affiliate networks must be encrypted. The CU Medicine and Affiliate networks are considered to be private and secure; therefore, sensitive data transmitted within these networks does not require encryption. Workforce members must use encryption when transmitting sensitive data over the Internet or any other open electronic communications network.

- SafeMail is the product CU Medicine uses to encrypt email. The instruction document for this tool is available on the CU Medicine corporate intranet website. Please contact the CU Medicine Help Desk (303-493-8000) for assistance or more information regarding encryption requirements and options.

University of Colorado Medicine
Information Security Workforce Summary

I have read, understand, and agree to follow the guidelines and policies reflected in this document.

_____

Employee Name (Print)

_____ _____

Employee Signature **Date**

_____ _____

Title **Department**

Employment Type (Select or Circle): ◯ **Employee** ◯ **Intern/Extern** ◯ **Temporary Staff** ◯ **Contractor/Consultant**

Please return completed forms to:

University of Colorado Medicine
Information Services Department
Attn: CU Medicine Help Desk
Box A069

Email: helpdesk@cumedicine.us