University of Colorado **Anschutz Medical Campus**

Campus Administrative Policy

Policy Title **Bring Your Own Mobile Device**

Policy Number: 4033A Functional Area: Human Resources

Effective:	April 26, 2023
Date Last Amended/Reviewed:	N/A (New Policy)
Date Scheduled for Review:	July 1, 2030
Supersedes:	N/A
Approved by:	Donald M. Elliman, Jr. Chancellor, University of Colorado Anschutz Medical Campus
Prepared by:	Office of University Counsel
Reviewing Office:	Executive Vice Chancellor of Administration and Finance and Chief Financial Officer CU Anschutz Office of Information Technology
Responsible Officer:	Executive Vice Chancellor of Administration and Finance and Chief Financial Officer
Applies to:	CU Anschutz Medical Campus

A. Introduction

University of Colorado Anschutz Medical Campus ("the University") recognizes that university employees at times utilize their personal Mobile Devices when conducting University business. In response to an increase in personally owned Mobile Devices being used in the work environment, the University has established an official Bring Your Own Device (BYOD) policy. Nothing in this policy requires a department or the University to compensate those who utilize their own personal devices. BYOD is the act of using a personal Mobile Device for University work- or business-related

activities. Employees who use their personal Mobile Devices for University work- or business-related activities must abide by the policy below.

B. Definitions

1. **Data Encryption** means securing data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext.
2. **Mobile Device** means cellular smartphones, tablets, notebook computers or any employee-owned device that the employee utilizes for University related communications, access data or confidential information.
3. **Personally Identifiable Information** means any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
4. **Sensitive Information** means any information that can be used to identify a person. Examples include personal information, medical records, financial information, University administrative computer data (employee records, student records, electronic documents that contain confidential information), passwords and account details, and research data. This includes information protected by The Family Educational Rights and Privacy Act (FERPA) and HIPAA.

C. Policy Statement

1. Purpose

The purpose of this policy is to outline the responsibilities and obligations of a University employee who participates in the BYOD program. This policy defines the acceptable use and procedures for using personally owned Mobile Devices, the storage and transmission of sensitive data, confidential and highly confidential data, and an employee’s obligation to maintain University related communications on a secure, University owned system.

Users must also comply with and adhere to Campus Administrative Policy 5001: Acceptable Use of Information Technology Policy, 5001: Acceptable Use of Information Technology Policy

This policy does not create a records retention requirement and employees must follow the University records retention policy and any hospital records retention policy that might apply. Retention of University Records

2. Responsibility

The University is not responsible for the purchase or costs associated with use of employee-owned Mobile Devices. The University is not responsible for technical support or repair of employee-owned Mobile Devices. The employee is responsible for providing the device and complying with this policy.

Expectations and Acknowledgements

Employees who participate in the BYOD policy must:

a. Not store any University communication, University data or University intellectual property exclusively on personally owned devices.

b. Must appropriately secure and encrypt the device.

c. Notify their department and the University of any theft or loss.

d. Notify their department and the University of any change in telephone number, if applicable.

e. Comply with local laws while operating a motor vehicle if conducting University business via cell phone.

f. Abide by all applicable laws set forth by Federal, State and Local Governments.

Employee acknowledges that:

a. All communications related to University business are public records as defined by the Colorado Open Records Act (CORA), Title 24, Article 72. Patient records, including Secure Chat (which is a part of the Epic record) are not a public record under CORA, but are still subject to other legal action such as subpoena or court order.

b. As a condition of using a Mobile Device to perform University business that any and all University related communication, data and work performed on a Mobile Device will be stored on a secure, official University system that can be accessed as necessary by the University to perform business including, but not limited responding to open records requests or other official requests, including a subpoena and any personnel related investigations related to employee's performance.

    - If an official request is made, text (SMS) messages must be electronically extracted and submitted to the requesting entity.

c. The employee has the obligation to secure and safeguard personally identifiable information and sensitive information, including the Health Insurance Portability and Accountability Act (HIPAA). If handling such data, the employee agrees to utilize encrypted forms of communication to transmit. Regarding safeguarding data, the employee must follow the University's Acceptable Use of Information Technology Policy Number 5001

d. If using a personal Mobile Device for transmitting or communicating patient information, Personally Identifiable Information, or Sensitive Information employee agrees to use Data Encryption applications to protect confidential and sensitive information including but not limited to protected health information and social security numbers.

3. Procedures

Violation of this policy or other university information technology policy can result in corrective and/or disciplinary action under applicable University or Board of Regents rules, regulations, policies, or collective bargaining agreements.

Notes

1. Dates of official enactment and amendments:

April 26, 2023: Approved by the CU Anschutz Chancellor

2. Initial Policy Effective Date: April 26, 2023

3. Cross References:
   - Campus Policy 5001: Acceptable Use of Information Technology Resources
   - CU System Administrative Policy Statement 2006: Retention of University Records