UMass Chan MEDICAL SCHOOL

# Encryption Policy

POLICY **07.01.06**

Effective Date: 08/01/2015
Last Revised Date: 05/14/2025
Last Review Date: 05/14/2025

**The following are responsible for the accuracy of the information contained in this document.**

**Responsible Policy Administrator**
Information Security Officer

**Responsible Department**
Information Technology

**Contact** UMassChanInformationSecurity@umassmed.edu

## Policy Statement

Schools, departments, and business functions are required to apply University-approved encryption solutions to preserve the confidentiality and integrity of, and control accessibility to, University of Massachusetts Chan Medical School (UMass Chan) data classified as Highly Restricted or Confidential* where this data is processed, stored or transmitted.

* Refers to Data Classification policy 07.01.03

## Reason for Policy

The purpose of this policy is to establish: the types of data, devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software and techniques used for encryption.

## Entities Affected By This Policy

This policy affects all department heads, chairs, faculty, and staff responsible for ownership or oversight of UMass Chan data, as defined by the Data Classification Policy.

## Related Documents

- Acceptable Use Policy (07.01.01)
- Data Classification Policy (07.01.03)

## Scope

UMass Chan Information is any information maintained by or on behalf of UMass Chan that is used in the conduct of UMass Chan business, regardless of the manner in which such information is maintained or transmitted. UMass Chan information formats include, but are not limited to, oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium.

## Responsibilities

Users who work with UMass Chan data must encrypt their data to prevent unauthorized disclosure.

Researchers who work with UMass Chan data approved by their respective IRB must encrypt their data to prevent unauthorized disclosure.

## Requirements

1. All databases that contain UMass Chan data Highly Restricted or Confidential data must encrypt the data at rest, with the exception of those UMass Chan resources housed in approved restricted-access facilities such as UMass Chan data centers.
    a. If there are contractual requirements for data at rest, data must be encrypted.
    b. All databases, application servers and file systems that contain UMass Chan Highly Restricted or Confidential data must leverage appropriate network access controls to ensure that access to the data is limited to those whose job functions require access.
2. Servers must not be directly accessible from the Internet or from publicly facing servers of the UMass Chan networks unless the information is encrypted.
    a. Information may be accessed remotely through an approved VPN connection. The use of an approved VPN is not considered direct access.
    b. UMass Chan Highly Restricted and Confidential Information must be encrypted when it traverses any network outside of the UMass Chan network.
3. Encryption is required for all laptops, workstations, mobile devices, and portable drives that may be used to store or access UMass Chan data.
    a. Laptops and Desktops that access third-party data (i.e., UMMHC) must comply with all data protection and encryption policies of the third-party.
    b. Departments who have a laptop, workstation, mobile device, or portable drive that needs to be encrypted must contact the UMass Chan Information Technology Help Desk.
4. All electronic messages containing UMass Chan Highly Restricted or Confidential data that are transmitted to any entity, institution, or group outside of the UMass Chan secured network must apply appropriate levels of encryption.
    a. Portal-based encryptions Transport Layer Security (TLS) and Secure File Transfer Protocol (SFTP) are acceptable encryption methods for message transmission.
5. Backups that contain UMass Chan Highly Restricted or Confidential data must be encrypted when stored outside of secured, primary locations.
6. Information can be stored on external devices with specific requirements and approval:

a. All portable media (including portal disk or thumb drives) containing UMass Chan Highly Restricted or Confidential data must be encrypted and a list of individuals with access to the media must be provided.
b. The device must be stored in a locked container when left unattended.
c. Whole disk encryption services are available for both Windows and Macintosh desktop and laptop computers as well as mobile devices such as external hard/flash drives.

## Definitions

Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized individuals. Encryption is a very important tool to safeguard protected and confidential data, but it is a powerful tool that needs to be installed and used with caution.

## Approvals

DocuSigned by:
Brian Coleman
232D95E3184B416...
Responsible Policy Administrator

6/26/2025
Date

Executive Vice Chancellor for
Administration & Finance

6/26/25
Date