Administrative Policy
2011-01 Data Encryption, Authentication and Physical Safeguards

Title	Data Encryption, Authentication and Physical Safeguards
Policy Owner and Contact Information	Information Technology Security itsecurity@uchc.edu / UConn Health Service Desk 860-679-4400
Applies to	All UConn Health workforce members, including employees, faculty, staff, students, residents, volunteers and other individuals.
Campus Applicability	UConn Health
Effective Date	12/16/2020

PURPOSE:
To establish requirements for the protection of confidential electronic data from improper alteration or destruction, including mechanisms to ensure that the confidential electronic data have not been altered or destroyed in an unauthorized manner.

APPLIES TO:
This policy applies to all UConn Health workforce members, including employees, faculty, staff, students, residents, as well as volunteers and other individuals with access to UConn Health systems.

This policy also applies to all forms of confidential electronic data maintained or transmitted by UConn Health.

DEFINITIONS:
Electronic resources are computing and telecommunications devices that can execute programs or store data which may include but are not limited to computers, mobile computing devices and storage devices (USB or otherwise connected).

POLICY STATEMENT:
Data Encryption
Confidential electronic data shall be encrypted while stored on electronic resources wherever available and feasible or whenever deemed necessary by risk analysis or evaluation.

Confidential electronic data shall be encrypted while in transit across an open communications network and transmitted using an approved secure file transfer product or protocol determined by the UConn Health Information Security Office.

All other confidential electronic data transmissions, e.g. client/server connections, shall be encrypted using approved mechanisms, e.g. virtual private networks, whenever available and feasible, or whenever deemed necessary by the risk analysis or evaluation.

Data Authentication

Confidential electronic data integrity shall be sustained using approved mechanisms, e.g. hashing algorithms, electronic signatures and digital signatures, whenever available and feasible or whenever deemed necessary by the risk analysis or evaluation.

Physical Safeguards

Electronic resources shall be secured using physical safeguards for protection of unauthorized access.

Screen locks, e.g., session timeouts, auto logoff, with password controls shall be activated on electronic resources.

Electronic resources shall be physically secured when not in use.

Monitors and screens displaying confidential information shall be physically placed in such a way that confidential information cannot be viewed by unauthorized individuals.

Electronic resources used to store confidential information must be reformatted/wiped using industry standards prior to disposal or reuse.

REFERENCES:

45 C.F.R. § 164.312(c) (1)
45 C.F.R. § 164.312(c) (2)
45 C.F.R. §164.312(e) (2)
45 C.F.R. §164.310

RELATED POLICIES:

2002-43 Confidentiality

ENFORCEMENT:

Violations of this policy or associated procedures may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, the University of Connecticut Student Code, other applicable University Policies, or as outlined in any procedures document related to this policy.

APPROVAL:

Andrew Agwunobi (Signed)	12/16/2020
UConn Health Chief Executive Officer	Date
Kiki Nissen (Signed)	12/15/2020
Administrative Policy Committee Vice-Chair	Date
Janel Simpson (Signed)	12/15/2020
Administrative Policy Committee Chair	Date

POLICY HISTORY:
New Policy Approved: 2/8/2011
Revisions: 12/16/2020 and renamed from UCHC Info Security: Data Authentication, Physical Safeguards
Replaces: 2005-01 UConn Health HIPAA IT Security: Data Authentication, Physical Safeguards on 2/8/2011.