UCONN HEALTH

POLICY NUMBER 2014-04
February 17, 2015

POLICY: SANCTIONS POLICY FOR PRIVACY AND SECURITY VIOLATIONS FOR FACULTY AND STAFF

The following data classification and definition shall be used:

Confidential data – Includes, but is not limited to, personally-identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual and/or the institution. Such harm might include but is not limited to:

- actions resulting in significant, severe or catastrophic harm to individuals;
- causing a significant or severe degradation in mission capability;
- causing significant or major damage to organizational assets;
- actions resulting in significant or major financial loss; or
- actions resulting in sanctions against UConn Health by a governmental or regulatory body.

Examples of such data may include, but are not limited to:

- Certain student information
- Medical/Dental/Behavioral Health-related patient information (PHI)
- Other sensitive UConn Health information not in the public domain
- Financial information (budgets, strategic revenue plans, accounts receivable/payable details) **NOTE: Credit card numbers are not to be collected, transmitted, or stored on UConn Health's computing devices and networks under any circumstances.** Posting credit card information to a vendor website for authorized purposes using UConn Health's computing devices is allowed. Sending credit card information via email for any reason is not allowed. For any questions please contact the Information Security Office.
- Employee human resources and financial information
- Any information about employees, students, patients, Board Members, etc. that includes Social Security numbers
- IDs and/or Passwords for access to UConn Health computing resources
- Research data requiring protections (clinical trials, patient survey responses, etc.) as required by federal and non-federal sponsors.

The data above is hereafter referred to as "Confidential Data" in this policy.

PURPOSE:
UConn Health policies regarding privacy and security of Protected Health Information (PHI) and other "Confidential Data" as a result of doing business, reflect its commitment to protecting the confidentiality of all forms of data whether on paper, in electronic form, or discussed verbally. While a commitment to privacy and security of data is an expectation, there remains a possibility that an inappropriate or unintended disclosure of any type of "Confidential Data" may result in a privacy breach. This policy will determine the procedure to manage and mitigate all breaches, both willful violations and unintended actions. This policy is also intended to be consistent with guidance described by the HIPAA and HITECH rules when managing patient information breaches.

SCOPE: This policy applies to the following members of UConn Health:

- Employees (including faculty and staff)
- Volunteers
- Temporary staff
- Agency and contracted staff
- Credentialed staff
- Members of the Board of Directors
- UConn Health sponsored business affiliates subject to a remote access agreement

Note: Students, fellows and residents please see Education policy in applicable handbook.

POLICY STATEMENT:
All forms of data in use whether created, obtained and/or owned by UConn Health are a valuable asset and must be protected from all known security and privacy risks which include unauthorized access, use, disclosure, modification, destruction, and removal. All forms of data are covered by this policy, including but not limited to: paper, any systems used to capture electronic data, as well as any media used for creating, obtaining or capturing data.

Disciplinary Sanctions and Appeals - Employees:

1. When a privacy and/or security violation is verified, existing UConn Health procedures for disciplinary action shall be used. Determination of appropriate process should include consultation with the Department of Human Resources - Labor Relations and other offices as appropriate.

2. Sanctions may include, but are not limited to:

    - Counseling
    - Oral Warning
    - Written Reprimand
    - Suspension
    - Termination

Business Associates and Sponsored Business Affiliates:

If the individual responsible for the violation/breach is a Business Associate or Sponsored Business Affiliate, UConn Health will take reasonable corrective steps to implement sanctions. While UConn Health is not required to monitor the activity of these partners, we will address problems as we become aware of them and request that they remedy their behavior. UConn Health reserves the right to terminate contracts if it becomes clear that the business partner cannot be relied upon to maintain the privacy/security of information we provide to them.

The remainder of this page intentionally left blank

UConn Health
Examples of Actions in Response to Privacy and Security Violations by Faculty and Staff

Level of Violation	Cause/ Motivation	Type of Violation	Examples of Violations	Examples of Possible Actions (one or more, not all-inclusive)
Level 1 Errors in handling "Confidential Data" or in maintaining security measures to protect that data	• Unintentional • Lack of training • Inexperience • Poor judgment • Poor process	Error based: • Clerical • Process • Technical • Judgment	• Sending "Confidential Data" to wrong postal, fax, or email address • Leaving an active computer screen with access to "CONFIDENTIAL DATA" unattended • Leaving "CONFIDENTIAL DATA", in any format, unattended in public areas • Disclosing "CONFIDENTIAL DATA" without identity verification • Discussing "CONFIDENTIAL DATA" in public or other inappropriate areas	• Letter of expectations, including provisions for mitigation, if appropriate • Inclusion of expectations/ mitigation steps on performance evaluation • Repeat of HIPAA Privacy & Security or other Training • Discussion of policy and procedures • Formal written counseling, verbal or written warning or reprimand • New Confidentiality Agreement signed • In research related violations, the AVP of Research Compliance would be notified and consulted regarding appropriate actions
Level 2 Breach in access, use or disclosure of "Confidential Data" and/or in maintaining security measures to protect that data	• Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness	• Unauthorized • Non-job related • Stealth	• Failure to properly dispose of paper and electronic media appropriately • Failure to implement appropriate safeguards for electronic "CONFIDENTIAL DATA" • Failure to complete required Security and Privacy Training and/or to sign appropriate Confidentiality Agreements • Accessing the medical /dental record of any person, including coworkers, friends, or family, without specific work-related need-to-know • Using someone else's computer account (not reporting lost password or MCD) • Installing unauthorized software with potential to harm systems • Adding, deleting, or altering electronic information without authorization • Unauthorized access to networks, servers, computer systems, or facilities/equipment rooms housing computer systems/servers • Failure to report a security or privacy violation • Failure to encrypt required electronic devices • Failure to establish a HIPAA Business Associate Agreement when needed • Failure to follow Special Restrictions for Out-of-Pocket Payment for Services under HIPAA/HITECH • Sharing password • Repeated Level 1 violations	• Written warning or reprimand, For faculty, referral to Department Chair for review and possible action; referral to Medical Staff Office for review and possible action • Restriction of information system user privileges • Suspension of employment • Restriction of participation in research projects or specific aspects of participation in research. The AVP of Research Compliance would be notified and that office would consult on possible actions up to and including suspension or termination of participation. If the violation involves research misconduct, further actions as per UConn Health Policy 2011-41 Research Misconduct may apply • Referral to police for investigation of potential crime.
Level 3 Breach in access, use or disclosure of "Confidential Data" and/or in maintaining security measures to protect that data for personal gain or to affect harm on another person	• Malicious intent • Financial gain • Revenge • Protest • Gross negligence	• Theft, including identity theft • Malicious actions: i.e., alteration or deletion of data; making systems inaccessible	• Access and unauthorized disclosure of "CONFIDENTIAL DATA" for personal gain or to affect harm on another person • Unauthorized access of celebrity or VIP HIPAA PHI/PII for any reason • Malicious alteration, deletion or removal of "CONFIDENTIAL DATA", from University facilities • Malicious introduction of known viruses, worms, Trojan horses or other malicious software into the organization's computer systems. • Unauthorized publication or broadcasting of "CONFIDENTIAL DATA" • A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline • Repeated Level 1 or 2 violations	• Suspension of employment • Suspension of Research Projects see above • Termination of information system user privileges see above • Referral to medical staff corrective action procedures • Termination of employment • Referral to police for investigation of potential crime. • The AVP of Research Compliance would be notified and that office would consult on possible actions up to and including suspension or termination of participation. If the violation involves research misconduct, further actions as per UConn Health Policy 2011-41 Research Misconduct may apply

Reference(s):

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) at 45 C.F.R. § 164.308; § 164.530
- The HITECH Act as amended in § 164.402 (2) (i)-(iv)
- Confidentiality Policy 2002-43
- UConn Health Information Security Policies
- Connecticut General Statutes § 36a-701b

Thomas Murphy (Signed) 3/10/15

Thomas Murphy **Date**
Chief Information Security Officer

Iris Mauriello (Signed) 3/10/15

Iris Mauriello **Date**
Compliance Integrity/Privacy Officer

Andrew Agwunobi (Signed) 3/11/15

Andrew Agwunobi, M.D., M.B.A. **Date**
Interim Executive Vice President for Health Affairs

New Policy: 2/17/15
Replaces Portions of Policy 2003-09