UCONN HEALTH

POLICY NUMBER 2003-31
February 17, 2015

POLICY: DATA CLASSIFICATION AND USE POLICY (Privacy & Security of Electronic Information)

PURPOSE:
To identify the data classification categories for all forms of data in use at UConn Health and to identify the responsibilities of individuals entrusted with this data.

SCOPE:
This data classification policy is applicable to all forms of data created, obtained, used, accessed, transmitted or stored at UConn Health. This policy is not intended to replace any applicable laws/regulations and applies to the following individuals:

- Employees (including faculty and staff)
- Volunteers
- Students and Residents
- Temporary Staff
- Agency and Contracted Staff
- Credentialed Staff
- Members of the Board of Directors

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.

The following data classifications and definitions 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.

Public data - Information obtained from the public domain or over which UConn Health wishes to exercise no proprietary rights or which has been released through official UConn Health channels. Public data requires no protective measures and no personnel are asked to exercise any particular actions according to this policy in support of this type of data.

RESPONSIBILITY:
It is the responsibility of each individual who is granted access to any of the data assets at UConn Health to exercise care in preventing unnecessary exposure of confidential data. In order to exercise care and prevent unnecessary exposure, each individual must adhere to all data security and privacy policies, standards and procedures and shall notify the appropriate management of any observed breach of security or privacy of data as required by law or UConn Health policies. Failure to follow established UConn Health policies may result in disciplinary action.

SECURITY ADMINISTRATION:
UConn Health Information Systems Security Office shall be responsible for the administration of all information security policies. The UConn Health Information Security Officer or his/her designee shall maintain these policies and shall establish standards and procedures for day-to-day implementation.

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: 4/13/03
Revised: 12/21/10, 2/17/15