UCONN HEALTH

POLICY NUMBER 2002-43
FEBRUARY 17, 2015

POLICY: CONFIDENTIALITY

POLICY STATEMENT:
This policy prohibits confidential information as defined by Federal, State of Connecticut and UConn Health policy from being accessed, disclosed or released in any format to or by any person/business that does not have a job related "need to know". In addition, certain information considered confidential by UConn Health may be subject to State of Connecticut Freedom of Information (FOI) but should not be released before obtaining specific authorizations from appropriate level of UConn Health management.

SCOPE:
Employees (including faculty and staff)
Volunteers
Students and Residents
Temporary Staff
Agency and Contracted Staff
Credentialed Staff
UConn Health Sponsored Business affiliates subject to remote access agreement

This policy covers all persons noted above during and after employment, volunteering, studying and/or when business with UConn Health has been completed or terminated.

DEFINITIONS:

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.

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

Conduct of Personnel: All individuals are expected to be professional and maintain confidentiality at all times, whether dealing with actual records, projects, or conversations, and abide by the obligations of contractual confidentiality agreements. Situations in violation of this policy include, but are not limited to:

a) Access, use, or disclosure of patient medical records, either paper or electronic, without a specific clinical purpose related to the treatment of the patient.
b) Access, use, or disclosure of patient medical records, either paper or electronic, for reasons other than treatment, payment, or healthcare operations.
c) "Loose" talk among healthcare workers regarding medical information about any patient or fellow employee, current or former.
d) Allowing unauthorized access on UConn Health computers to patient information, financial data, research data, or employee personal information.
e) Sharing of information acquired by persons in the course of their work to others who don't have a need to have the information; accessing information that the individual doesn't have the authority to access in the course of their work, or doesn't have a need to know to carry out their job duties.
f) Disclosure of the anonymity or medical information of research participants without the research subject's/legal representative's permission.
g) Sharing of information relative to confidential Human Resources matters.
h) Breach of confidentiality obligations regarding the disclosure of confidential information that is subject to a duly signed confidentiality or research agreement.
i) Discarding confidential documents in non-secured trash. (Secured shredder bins must be used).

Examples of Types of Information to be Protected:

1. **Patient Information:** Patient information must not be accessed, removed, discussed with or disclosed to unauthorized persons, either within or outside of the institution, without the proper consent of the patient. All individuals having access to confidential information are

bound by strict ethical and legal restrictions on the release of medical data. No individual therefore may disclose to a third party, including his/her own family, information learned from medical records, patient accounts, management information systems, or any other confidential sources during the course of his/her work. No individual may access confidential information that they do not have a need to know to carry out their job duties. Employees may not access, release or discuss the medical information of other employees without proper consent, unless the employee must do so to carry out specific assigned job functions. Employee patient information should never be accessed for employment reasons.

2. **UConn Health Information:** UConn Health information that must be protected includes but is not limited to:
   - Ongoing negotiations (labor contracts, leases, purchases)
   - Pending litigation and/or investigations
   - Information that is proprietary, e.g., information that allows UConn Health to be more competitive in the marketplace. For example: an innovative approach that is described in a grant proposal.
   - Confidential commercial or financial information

   This information may not be accessed, removed, altered or disclosed unless UConn Health administration has given proper authorization.

3. **Faculty, Employee and Student Information:** This includes personnel, medical, and any other files where unauthorized access, release or disclosure, falsification or destruction of individual records is strictly prohibited.

Disposal of Confidential Documents: Confidential documents must be disposed of utilizing the designated locked containers for shredding.

Reporting Breach of Confidentiality: Persons must report violations of this policy. Breaches of patient information or other confidential information must be reported to the UConn Health Privacy and Information Security Officers. Other reports may be made to a supervisor, Department Chairperson, Compliance Office, Privacy Officer, Information Security Officer or by calling the confidential "Reportline" at 1-888–685–2637.

Disciplinary Action for Non-compliance: Violation of this policy is cause for disciplinary action up to and including dismissal.

Andrew Agwunobi (Signed) 3/10/15

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

Replaces: Policy presented to Health Affairs Committee on September 1, 1994
Senior Group Approval June 27, 1994
Revised: 2/99, 10/00, 3/01, 8/02, 5/04, 7/14, 12/14, 2/15
Reviewed: 10/16/09