# HIPAA/PRIVACY AND SECURITY OF CONFIDENTIAL DATA

## CONFIDENTIAL DATA

The University of Connecticut School of Medicine (UConn SOM) and affiliated sites have policies and procedures governing the privacy and security of confidential data (including but not limited to patient's personal health information). These policies also establish requirements for the security and appropriately controlled release of all such information, consistent with applicable federal and state laws, including the federal privacy rule. Residents and fellows must abide by the policies and procedures governing privacy and security of confidential data at the University of Connecticut School of Medicine (UConn SOM) as well as at all affiliated sites.

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. (see UConn Health's Confidentiality Policy.)

In the course of the resident's/fellow's employment, the resident/fellow may be granted access to various types of *Confidential data*, including but not limited to:

- Patient information that is protected by both Connecticut and federal laws, such as the Health Insurance Portability Accountability Act ("HIPAA").
- Sensitive UConn Health information not in the public domain
- Financial information (budgets, strategic revenue plans, accounts receivable/payable details)
- IDs and/or Passwords for access to UConn Health computing resources
- Research data requiring protections

Security of *confidential data* is governed by policy on the acceptable use of electronic resources (see UConn Health's Acceptable Use Policy)

## PATIENT INFORMATION

Confidential patient information includes (but is not limited to) any information about health status, provision of health care, or payment for health care that is created or received by a resident/fellow, another medical professional, or a health care institution, and can be linked to a specific individual. This includes patient information in written, oral or electronic form.

Residents/fellows shall not access or disclose confidential patient information except as may be required by law and the applicable policies or procedures of any site in which the resident/fellow may train.

Residents/fellows have a responsibility to keep secure and confidential the information collected about patients during their encounters with healthcare professionals. Releasing parts or all of that information is appropriate under certain circumstances, such as when treating the patient, providing for continuity of care, participating in approved research and educational activities, complying with laws, and assuring reimbursement for services provided

UConn Health has specifically developed a policy to guide residents/fellows in the use of patient data for educational purposes. (see The Use of PHI in Education policy)

UConn Health's Privacy and Security Policies linked here provide guidance to residents/fellows to assure patient rights are protected:

https://health.uconn.edu/policies/policies-specific-areas/specific-area-hipaa-security/

Revised 4/16, 5/17, 9/17, 11/17, 4/19, 3/21
Reviewed 2/23