Administrative Policy

2003-09 Responding to Breaches of Privacy or Security of Protected Health Information (PHI) and/or Personal Information

Title	Responding to Breaches of Privacy or Security of Protected Health Information (PHI) and/or Personal Information
Policy Owner and Contact Information	Office of Healthcare Compliance and Privacy, privacyoffice@uchc.edu Information Technology Security, itsecurity@uchc.edu
Campus Applicability	UConn Health
Applies to	UConn Health Workforce, including John Dempsey Hospital, and Business Associates
Effective Date	March 30, 2023

PURPOSE:
To comply with certain provisions of the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and the associated regulations (collectively "HIPAA") and Connecticut and other state laws regarding reporting and responding to suspected or known incidents involving the privacy or security of Protected Health Information (PHI) and/or Personal Information, as applicable.

POLICY STATEMENT:
UConn Health promptly responds to and investigates suspected or known Breaches of privacy or security of PHI and/or Personal Information. UConn Health mitigates any known harmful effects of a Breach or other incident involving PHI and/or Personal Information to the extent practicable. UConn Health provides any notification(s) required by law, and applies appropriate sanctions against Workforce members who do not comply with its policies and procedures.

Internal Reporting
Workforce members must report promptly to the Office of Healthcare Compliance and Privacy (OHCP), the UConn Health Information Security Officer (ISO), or the University Reportline any suspected or known incident that raises concerns about the privacy or security of PHI and/or Personal Information.

Suspected or known incidents that raise concerns about the privacy or security of Confidential Data other than PHI and/or Personal Information should be reported to the UConn Health Information Security Officer (ISO) or the confidential REPORTLINE.

Investigating
The OHCP and/or the ISO, in consultation with the Office of the General Counsel and/or other departments as appropriate, will investigate known and suspected incidents involving the privacy or

security of PHI and/or Personal Information and will determine whether an incident is reportable under HIPAA or State law, or otherwise requires specific action based on the facts and circumstances.

Mitigation

UConn Health will mitigate, to the extent practicable, any known harmful effect of a Breach or other incident involving PHI and/or Personal Information that violates HIPAA, other laws or regulations, or UConn Health policies or procedures.

Breach Notification

In the event of a Breach, UConn Health will notify the affected individual(s), the Secretary of the Department of Health and Human Services, the media, and the Connecticut Office of the Attorney General and/or Attorneys General in other states as applicable, to the extent and within the timeframes required by law.

Documentation

UConn Health will maintain documentation demonstrating that all required notifications were made, or, alternatively, documentation demonstrating that notification was not required, for no less than six (6) years, or any longer retention period required by law (see 2003-02 Documentation and Retention of HIPAA Compliance Records).

Incidents Occurring at or by Business Associates or their Subcontractors

Business Associates of UConn Health are required by the Business Associate Agreement (BAA) to notify UConn Health of their or their subcontractor's discovery of any:

- use or disclosure of PHI not provided for in the BAA or underlying contract; or
- Breach; or
- Security Incident.

UConn Health may, in its discretion, delegate to the Business Associate investigation of any such incident and/or responsibility for providing Breach notification(s) to affected individuals and other required parties.

DEFINITIONS:

Privacy Definitions

Breach of Unsecured PHI (Breach): For purposes of this policy, a "Breach" of PHI shall have the same meaning as defined in 45 C.F.R. § 164.402.

Breach of Security: For purposes of this policy, a "Breach of Security" shall have the same meaning as defined in Conn. Gen. Stat § 36a-701b as amended by Section 1 of Public Act No. 21-59 An Act Concerning Data Privacy Breaches.

Personal Information: For purposes of this policy, "Personal Information" shall have the same meaning as defined in Conn. Gen. Stat. § 36a-701b as amended by Section 1 of Public Act No. 21-59 An Act Concerning Data Privacy Breaches.

Protected Health Information: For purposes of this policy, "Protected Health Information" shall have the same meaning as defined in 45 C.F.R. § 160.103.

Security Incident: For purposes of this policy, a "Security Incident" shall have the same meaning as defined in 45 C.F.R. § 164.304.

Workforce: For purposes of this policy, "Workforce" shall have the same meaning as defined in 45 C.F.R. § 160.103.

PROCEDURES/FORMS:
Procedures for Responding to Breaches of Privacy or Security of Protected Health Information (PHI)

REFERENCES:
45 C.F.R. §§ 164.308 and 164.530 (HIPAA Security and Privacy Rule)
45 C.F.R. §§ 164.400-414 (HIPAA Breach Notification Rule)
Conn. Gen. Stat § 36a-701b as amended by Section 1 of Public Act No. 21-59 An Act Concerning Data Privacy Breaches

RELATED POLICIES:
2002-43: Confidentiality
UConn Health Information Security Policies
2003-04: Business Associate Agreements
2014-04: Sanctions for Privacy and Security Violations

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:

Bruce Liang (Signed)_____ 3/30/2023_____
Bruce Liang — Date
UConn Health Chief Executive Officer

Kiki Nissen (Signed)_____ 3/30/2023_____
Kiki Nissen — Date
Administrative Policy Committee Vice-Chair

Janel Simpson (Signed)_____ 3/30/2023_____
Janel Simpson — Date
Administrative Policy Committee Chair

POLICY HISTORY:
Revised & Renamed: 1/28/05. Original policy name was "Sanctions for Breaches of Privacy & Security of PHI & UCHC's Duty to Mitigate Such Breaches" which was a new policy on 1/14/03.
Revised: 4/10, 9/13, 7/14, 3/23