

HIPAA PRIVACY AND SECURITY POLICY GUIDANCE

This guidance is for URI personnel who may encounter health-related information in University operations. HIPAA applies to certain URI departments and activities, but not to every University office, record, system, activity, or employee solely because health-related information is involved. Capitalized terms used but not defined herein shall be defined by the applicable statute or regulation from which they originated.

HIPAA Framework and Protected Health Information

HIPAA applies to covered entities and business associates that handle protected health information (“PHI”) in connection with HIPAA-regulated functions. A Covered Entity generally includes a health plan, health care clearinghouse, or health care provider that conducts covered transactions electronically. A Business Associate is a person, entity, department, program, or function that creates, receives, maintains, or transmits PHI to perform services or support functions for a covered entity or covered component.

Protected Health Information (“PHI”) means individually identifiable health information held or transmitted by a Covered Entity or Business Associate in any form or medium, including electronic, paper, or oral information. PHI includes identifiable information relating to an individual’s past, present, or future physical or mental health or condition, the provision of health care, or payment for health care.

Not all health-related information is PHI. HIPAA excludes certain categories of information, including student records covered by the Family Educational Rights and Privacy Act (“FERPA”) and employment records held by a Covered Entity in its role as employer. A record is not PHI solely because it references a medical condition, diagnosis, disability, leave issue, benefit, workplace accommodation, or wellness/fitness.

URI as a whole is not a covered entity because the University as a whole does not operate as a health plan, health care clearinghouse, or covered health care provider. Rather, URI has designated itself as a HIPAA hybrid entity, meaning HIPAA applies only to designated components that perform HIPAA-covered functions. HIPAA obligations depend on the function performed, the URI component involved, the role of any Business Associate, and whether the information being handled is PHI, and therefore, covered by HIPAA.

Designated HIPAA Components

URI’s designated Health Care Components are: (1) URI Health Services, (2) URI Emergency Medical Services, (3) University Physical Therapy, and (4) URI Speech and Hearing Centers. URI’s designated (internal) Business Associate Components are: (1) the URI Office of Information Technology Services and (2) the URI Office of the Chief Information Security Officer. Therefore, HIPAA only applies to these covered components.

If a unit is not a designated Health Care Component or Business Associate Component listed above, HIPAA generally does not apply to that unit even if it handles health-related information. However, other laws, University policies, contractual obligations, or confidentiality requirements may still apply.

Student, Employment, and Administrative Health Information

Student health records are generally governed by FERPA rather than HIPAA. FERPA regulates the privacy, use, and disclosure of student records, and HIPAA generally does not apply to URI student health records because HIPAA excludes FERPA-covered records from the definition of PHI.

THE UNIVERSITY OF RHODE ISLAND

Employment-related health information is also not automatically subject to HIPAA. Individually identifiable health information maintained by URI in its role as employer, including Human Resources records for employment, accommodation, workers' compensation, or personnel purposes (e.g. health information received under the Americans with Disabilities Act or the Family and Medical Leave Act or through a workers' compensation claim) is generally excluded from PHI under HIPAA.

Research and Contract Review

Research involving health-related information is not automatically subject to HIPAA solely because it involves health, medicine, treatment, diagnosis, wellness, clinical outcomes, surveys, or similar topics. HIPAA may apply when research involves PHI from a URI Health Care Component or Business Associate Component, PHI from another Covered Entity, a Business Associate, HIPAA authorization or waiver, a limited data set, preparatory-to-research access, decedent information that remains PHI, or HIPAA-related contract terms. Before University records are accessed, used, or disclosed for research, URI must determine whether the records are PHI. Research protocols are in place with the URI Office of Research Integrity (ORI) for that process and determination.

Business Associate Agreements (BAAs) are required when a party provides data transmission services to URI involving PHI, requires routine access to PHI, or creates, receives, maintains, or transmits PHI on behalf of a URI Health Care Component. A Data Use Agreement may be required when a limited data set or other HIPAA-regulated data set is used or disclosed for research, public health, health care operations, or another permitted purpose. Agreements involving PHI, limited data sets, HIPAA, HITECH, security requirements, breach reporting, re-identification restrictions, downstream data protection obligations, or similar HIPAA-related terms must be reviewed and approved by the HIPAA Privacy Officer, in consultation with the Office of General Counsel, before execution. URI maintains its own BAA forms that must be used in any situation deemed to require a BAA after such consultation.

Rhode Island Law and Escalation

The Rhode Island Confidentiality of Health Care Communications and Information Act ("RI-CHCCIA") may apply alongside FERPA or HIPAA and may also apply where neither federal law applies. Where HIPAA and state requirements differ, and unless preempted, URI strives to apply the law most protective of patient privacy in the particular circumstance.

HIPAA Compliance Oversight at URI

As required by the HIPAA Regulations, URI has appointed the following individuals to serve as URI's HIPAA Privacy and Security Officers:

1. URI HIPAA Privacy Officer: Associate Director
URI Health Services
2. URI HIPAA Security Officer: Chief Information Security Officer
URI Information Technology Services

Individuals in these roles are responsible for carrying out duties as described in the Policy on HIPAA Privacy and Security.