THE
UNIVERSITY
OF RHODE ISLAND

Policy on HIPAA Privacy and Security

Policy Title	Policy on HIPAA Privacy and Security
Policy #	01.114.1
Policy Owners	Provost and Executive Vice President for Academic Affairs; Vice President for Student Affairs.
Contact Information	Questions regarding this policy can be directed to the Associate Director of Health Services at 401-874-5155 or the Chief Information Security Officer at 401-874-4787.
Approved By	President of the University
Effective Date	June 26, 2026
Next Review Date	No later than June 30, 2031
Who Needs to Know About this Policy	All University of Rhode Island (University) faculty, staff, and students; University Affiliates; and third parties who access, create, receive, maintain, or transmit protected health information.
Definitions *Defined terms and shorthand references are capitalized throughout.*	**Business Associate.** A University college, department, program, clinic, or function, or a third-party person or entity engaged by the University, that creates, receives, maintains, or transmits PHI to perform certain functions or activities on behalf of a University Health Care Component, or provides any function that involves access of PHI. **Covered Entity.** Any health plan, healthcare clearinghouse, or healthcare provider that transmits PHI in electronic form in connection with a covered transaction. **Covered Transaction.** The transmission of information between two parties to carry out financial or administrative activities related to healthcare and includes: healthcare claims or equivalent encounter information; healthcare payment and remittance advice; coordination of benefits; healthcare claim status; enrollment and disenrollment in a healthcare plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; healthcare electronic funds transfers (EFT) and remittance advice; or other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation. **Health Care Component.** Any University college, department, program, clinic, or function that: (1) meets the definition of HIPAA Covered Entity, if it were a separate legal entity; (2) performs Covered Functions; or (3) for purposes of this policy is a Business Associate. These components are designated by the Hybrid Entity in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(C). **Hybrid Entity.** A single legal entity that conducts both HIPAA-covered and non-covered functions as part of its business and designates Health Care Components in accordance with HIPAA.

	Protected Health Information ("PHI"). Individually identifiable health information held or transmitted by a Covered Entity or its business associate, in any form or media, whether electronic, paper, or oral. PHI is information, including demographic data, that relates to: ● The individual's past, present or future physical or mental health or condition; ● The provision of health care to the individual; or ● The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. PHI excludes individually identifiable health information: 1) Covered by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99) ("FERPA"); 2) In employment records held by a Covered Entity in its role as employer; and 3) Regarding a person who has been deceased for more than 50 years. **Workforce Members.** University Employees, authorized volunteers, trainees, students, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such entity, whether or not they are paid by the Covered Entity.
Statutes, Regulations, and Policies Governing or Necessitating This Policy	21st Century Cures Act (Cures Act), 42 U.S.C. § 300jj-52 (Information Blocking), and implementing regulations at 45 C.F.R. Parts 156, 406, 410, 411, 422, 431, 457, 482, and 485. Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17901–17953. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §§ 1320d–1320d-9 (Standards for Privacy of Individually Identifiable Health Information), and implementing regulations at 45 C.F.R. Parts 160 and 164. R.I.G.L. § 5-37.3 et seq. (Rhode Island Confidentiality of Health Care Communications and Information Act (RI-CHCCIA)).
Reason for Policy/Purpose	This policy is intended to provide Workforce Members clear expectations for compliance with health information privacy and security requirements.
Forms Related to this Policy	HIPAA Compliance Program (Restricted)

Policy Statement

The University of Rhode Island ("University") maintains a HIPAA Compliance program (the "HIPAA Compliance Program") to guide compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the 21st Century Cures Act ("Cures Act"), and the Rhode Island Confidentiality of Health Care Communications and Information Act ("RI-CHCCIA") as they relate to the privacy and security of health information. HIPAA and HITECH provide the foundational framework, establishing national standards for protecting PHI of non-students, defining the

responsibilities of Covered Entities and Business Associates, and setting security requirements for electronic healthcare transactions. The Cures Act builds upon HIPAA by promoting interoperability across electronic health record systems and enhancing individuals' rights to access their electronic health information without unnecessary barriers. The RI-CHCCIA establishes state-level protections specific to safeguarding healthcare information that relates to an individual. Together, these regulations provide individuals with robust rights to access and control their health records while mandating safeguards to protect the confidentiality and integrity of healthcare information. Where federal and state requirements differ, the University applies whichever law is most protective of patient privacy in any particular circumstance, unless preempted by federal law.

Student health records are generally governed by FERPA rather than HIPAA. FERPA regulates the privacy, use, and disclosure of these records and preempts conflicting state laws. Additional information can be found in the University's *Policy on the Rights of Students Pursuant to FERPA*.

I. Scope and Applicability

The University conducts a broad range of HIPAA-covered and non-HIPAA covered functions and activities, including certain healthcare services that are subject to federal and state privacy and security regulations. In compliance with governing regulations, the University has implemented and maintains administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI within the scope of this policy. Specific procedures, standards, and implementation specifications for each safeguard category are documented in the University's HIPAA Compliance Program (Restricted) and corresponding Health Care Component and Business Associate privacy and security protocols.

The University has designated itself as a Hybrid Entity. As such, the University has identified the Health Care Components that perform Covered Transactions and the Business Associates that provide covered services for Health Care Components. HIPAA does not apply to all University offices, departments, programs, activities, records, or systems solely because they involve health-related information. All Workforce Members, and all individuals who create, receive, maintain, transmit, use, disclose, access, or may encounter PHI on behalf of a University Health Care Component or Business Associate , are required to comply with the University's HIPAA Compliance Program.

For purposes of this policy, health-related information that is not PHI, even though it relates to health, illness, disability, benefits, leave, accommodations, wellness, fitness, or similar topics, is not covered by HIPAA or this policy. For example, individually identifiable health information maintained by the University in its role as employer, including by Human Resources for employment, accommodation, workers' compensation, or personnel purposes, is generally not PHI under HIPAA, although other laws, policies, contractual obligations, or confidentiality requirements may apply. Student health records are generally governed by FERPA rather than HIPAA, and additional information can be found in the University's Policy on the Rights of Students Pursuant to FERPA. Questions about whether a particular record, activity, system, contract, disclosure, office, or department is subject to this policy should be directed to the HIPAA Privacy Officer or HIPAA Security Officer, as appropriate.

II. Roles and Responsibilities

The University has designated a HIPAA Privacy Officer and a HIPAA Security Officer. They are accountable for developing, implementing, maintaining, and enforcing the University's HIPAA Compliance Program. Their responsibilities, though distinct, collectively include monitoring compliance, providing Workforce Member training, conducting risk assessments, managing incident response for security breaches, handling patient rights requests and privacy complaints, and other activities outlined in the HIPAA Compliance Program.

Each University Health Care Component is required to designate a "HIPAA Compliance Lead" to assist the HIPAA Privacy and Security Officers in implementing, monitoring, maintaining and enforcing HIPAA compliance within the

Health Care Component and with any Business Associates of the component. The HIPAA Compliance Lead shall serve as the Health Care Component's primary compliance liaison, facilitate communication with the Privacy and Security Officers, and communicate with Workforce Members so they are aware of and comply with the University's HIPAA Compliance Program. The HIPAA Compliance Lead, in collaboration with the Privacy and Security Officers, shall identify any suspected compliance gaps and recommend corrective actions. Notwithstanding, all Workforce Members share responsibility for HIPAA compliance and shall promptly report potential violations or other concerns to the HIPAA Compliance Lead or Privacy and Security Officers.

III. Security and Risk Assessment

To protect the confidentiality of electronic PHI created, received, maintained, or transmitted by the University, each Health Care Component shall strive to meet or exceed standards set in the HIPAA Security Rule. The standards include implementing appropriate and reasonable administrative, physical, and technical security measures sufficient to reduce risks and vulnerabilities. Such measures will be implemented based on the level of risks, capabilities, and operating requirements of each Health Care Component. The University shall conduct security risk assessments of all systems that create, receive, maintain, or transmit electronic PHI as required by HIPAA, and the HIPAA Security Officer shall document findings, establish remediation plans, report results to the HIPAA Privacy Officer and University leadership, and monitor implementation of any necessary remediation activities.

IV. Business Associate Agreements

All University Health Care Components and Business Associates are required to enter into a Business Associate Agreement ("BAA") or Subcontractor BAA with any party that:

1. provides data transmission services to the University with respect to PHI and/or requires access on a routine basis to PHI; or
2. creates, receives, maintains, or transmits PHI on behalf of a University Health Care Component.

The BAA establishes the privacy and security obligations, permitted uses, and required safeguards for any third party that creates, receives, maintains, or transmits PHI on behalf of a University Health Care Component. Any third-party BAA, Subcontractor BAA, or other agreement that permits a third party to create, receive, maintain, transmit, use, disclose, or access PHI on behalf of the University must be reviewed and approved by the HIPAA Privacy Officer, in consultation with the Office of General Counsel, before execution. Unless otherwise approved by the HIPAA Privacy Officer, in consultation with the Office of General Counsel, all BAAs must be executed on a University BAA contract templates maintained by the HIPAA Privacy Officer and shall be subject to any other applicable University policies or department protocols related to University contracts and other binding documents.

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. A Data Use Agreement is not a substitute for a BAA when a third party creates, receives, maintains, transmits, uses, discloses, or accesses PHI on behalf of a University Health Care Component or Business Associate. Any Data Use Agreement, data transfer agreement, research agreement, services agreement, reliance agreement, or other contract that involves PHI, a limited data set, 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.

V. Training Requirements

Workforce Members are expected to complete all required training as outlined in the University's HIPAA Compliance Program and otherwise communicated to them by the University's HIPAA Privacy and Security Officers. Training

must be completed within designated timeframes, and supervisors are responsible for supporting and monitoring training participation by Workforce Members in compliance with this policy and the University's HIPAA Compliance Program.

VI. Reporting Violations and Security Incidents

All Workforce Members are expected to report any known or suspected HIPAA violations or PHI-related data privacy and security incidents to the University's HIPAA Privacy and Security Officers within two hours of becoming aware of the suspected violation or incident to enable prompt investigation, response and mitigation.

VII. Enforcement

Violations of this policy will be reported to the HIPAA Privacy and Security Officers for investigation, and may result in disciplinary action, up to and including termination. Intentional or repeated violations may result in additional sanctions or penalties commensurate with the severity of the violation and applicable law.

VIII. PHI in Research

Research activities intended to be conducted by, through, or on behalf of a University Health Care Component or Business Associates of the component that may create, review, maintain, transmit, use, or disclose PHI must be disclosed to the University's HIPAA Privacy and Security Officers before the PHI is accessed, used, disclosed, transferred, or incorporated into the Research so that compliance with this policy and applicable laws and regulations can be guided. "Research" includes all basic, applied, clinical, translational, demonstration and creative activities in all academic and scholarly fields including, but not limited to the arts, sciences, liberal arts, applied sciences, social sciences, and professions, including Research activities involving human subjects and animals. Research conducted outside of the University's Health Care Components is not within the scope of this policy; however, HIPAA or other laws, regulations, University policies, contractual obligations, or confidentiality requirements may apply if PHI is used for Research.

A URI researcher who requests PHI from a University Health Care Component or Business Associate must obtain review through the University's applicable HIPAA and research compliance processes before the requested PHI is accessed, used, disclosed, transferred, or incorporated into the Research.

Where PHI will be used or disclosed for research, the University will identify the applicable HIPAA pathway before the use or disclosure occurs.

Exceptions

None

Policy Review and Revisions

(Versions earlier than the first policy number may be paper only)

Policy #	Effective Date	Reason for Change	Changes to Policy
01.114.1	June 26, 2026	n/a	n/a