

Policy on Collection and Use of COVID-19 Related Health Screening and Safety Information

Policy Title	Policy on Collection and Use of COVID-19 Related Health Screening and Safety Information
Policy #	01.106.2
Policy Owners	URI Chief Information Officer and AVP for Student Health and Wellness
Contact Information	Questions about this policy should be directed to the University of Rhode Island CIO at (401) 875-4599 and/or AVP for Student Health and Wellness at (401) 874-5155
Approved By	Administrative Policy Committee
Effective Date	December 14, 2021
Next Review Date	No later than December 31, 2022
Who Needs to Know About this Policy	All faculty, staff, and students of the University as well as other Affiliates, vendors/contractors, and any other parties on campus who may use the IT resources of the University (including guest Wi-Fi access) while on any University Property.
Definitions	<p>University Affiliate. Any individual who is not a faculty member, staff, or student who otherwise has a formal relationship with the University, including but not limited to visiting scholars, visiting students, research fellows, professional program participants, club sports coaches, and volunteers as well as employees and associates of the URI Foundation and Alumni Engagement, URI Research Foundation, and members of the University of Rhode Island Board of Trustees. Vendors and contractors are not considered University Affiliates, except for those with an ongoing presence on the University campus as regular operations support staff.</p> <p>University Property. Property belonging to the State of Rhode Island and held in trust by the University of Rhode Island Board of Trustees; property held by the University of Rhode Island or any of its component units in its own name; and property owned by third parties but assigned to, occupied by, or managed by the University or any of its component units.</p>
Statutes, Regulations, and Policies Governing or Necessitating This Policy	<p>34 CFR Part 99; 20 U.S.C. 1232g (FERPA)</p> <p>45 CFR 164 (HIPAA)</p> <p>RIGL. § 5-37.3 (Rhode Island Confidentiality of Health Care Communications and Information Act)</p>

Reason for Policy/Purpose	To describe the collection and use of COVID-19 Related Health Screening and Safety Information by the University to protect the health and safety of all individuals on campus. This policy describes the types of COVID-19 Related Health Screening and Safety Information, including individual self-reported health status and symptom information, and individual campus location information that the University collects and maintains. It further describes the ways in which that data may be used by the University to protect the health and safety of all individuals on campus.
Forms Related to this Policy	None

Policy Statement

The University of Rhode Island is committed to providing and maintaining a healthy learning and working environment for all students, staff, faculty, and other members of the University's community. In order to help ensure a healthy and safe environment, the University may collect self-reported health information as well as information about an individual's presence on University Property, including their location on campus. Information collected and accessed by the University pursuant to this policy will generally be provided voluntarily by individuals, but in those cases where information provision by individuals is required, or (as in the case of location information) access to stored network information is accessed and used for the purpose of furthering the University's COVID-19 health and safety response, the use of the information is considered an appropriate and legally permissible administrative collection and use necessitated by the University's special needs in responding to the dangerous COVID-19 pandemic. The collection and use of health information and location information will be addressed separately as follows.

A. Health Information

The University will collect the following self-reported COVID-19 Related Health Screening and Safety Information from individual members of the University Community (i.e. employees, students, visitors, Affiliates): (1) Daily Self-Assessment Information (COVID-19 Health Symptom Screening) to be provided by individuals through the secure electronic information reporting and storage system established by the University; (2) other information reported to, or observed or obtained by, University officials relating to an individual's health status or symptoms (e.g., information that a student or employee on campus has been coughing or sneezing repeatedly); (3) COVID-19 virus test result information; (4) follow-up health status information such as additional self-reports of health status or symptoms, test reports, or healthcare provider information from individual employees, students, visitors, or Affiliates who have been determined (as a result of a Daily Self-Assessment or otherwise) to be at risk for COVID-19 and thus temporarily required to self-isolate or remain away from University Property; and (5) COVID-19 vaccine information, including vaccine exemption information.

The above-described COVID-19 Related Health Screening and Safety Information, relating to both students and employees, shall be maintained by URI Health Services in a secure system approved by Information Technology Services. Such information that relates to University employees will be considered HIPAA-exempt "employment records" held by URI "in its role as employer" and have the status afforded to such information under HIPAA. Such information that relates to URI students will be integrated with the other electronic health records maintained by URI Health Services for all URI students, all of which will continue to be treated as "educational record" information under FERPA.

In general, and subject to the limited exceptions described below, no personally-identifiable COVID-19 Related Health Screening and Safety Information collected and maintained by URI Health Services—other than information indicating that an individual has been determined to be “safe to be on campus” (“safety clearance information”)—will be shared with other University offices or officials outside of URI Health Services unless permission has been granted by the individual. The limited exceptions to the foregoing confidentiality limitation are that URI Health Services may, in limited circumstances, share personally identifiable COVID-19 Related Health Screening and Safety Information internally within URI or externally to third parties outside of URI, when (1) required by applicable law; (2) to ensure individuals are in compliance with University health and safety practices (e.g., required testing); or (3) as permitted by applicable law and deemed reasonably necessary for health or safety reasons (e.g., when required to report information to the Rhode Island Department of Health, when ordered to disclose information by a court, when internal disclosure to certain University personnel [“school officials,” per FERPA] is deemed necessary to meet the University’s needs to further its COVID-19 response health and safety plans, or when a disclosure to a healthcare provider or other party is necessitated by a medical or public safety emergency).

All COVID-19 Related Health Screening Safety Information about an individual shall be secured and maintained at all times by URI Health Services, URI Information Technology Services (and any other URI department or unit who may have obtained the information) in accordance, at a minimum, with the technical and physical security safeguards of HIPAA. Any COVID-19 Related Health Screening and Safety Information not directly retained in the electronic health records of URI Health Services will be permanently deleted as soon as this data is no longer required for safety and contact tracing purposes as defined by the CDC.

Where applicable, an individual’s Health Screening and Safety Information will generally be shared on a need-to-know basis with certain University officials outside of URI Health Services. In the case of employees, these individuals may include supervisors or Human Resources officials. For students, these individuals may include program leaders, supervising faculty, and student life officials. Entry into some areas of campus may require verification of attestation, vaccination, or proof of testing.

B. Location Information

Information about an individual’s location on campus may appear in any number of electronic records, including but not limited to network connection, software use, computer activity, ID badge swipes. The data collected by these systems may be monitored and analyzed by IT professionals employed by or contracted to the University of Rhode Island. These individuals are not authorized to disclose any of this information to anyone except as specifically listed in subsections (i) and (ii) below.

Aggregate statistics about program participation combined with other electronic indicators of presence on campus may be shared with relevant department heads, college leaders and divisional leaders to include all members of the Council of Deans and the Senior Leadership of the University, as well as relevant State of Rhode Island officials. In all cases reasonable efforts shall be made to ensure this information does not identify individual respondents.

(i) Personally Identifiable Data

Individually identifiable data may be disclosed to health services professionals for the purpose of identifying individuals who may have been exposed to health risks for the purposes of contact tracing and provisioning of health care related services (such as health checks, food delivery for individuals in quarantine, enhanced cleaning protocols, and similar services).

In addition, personally identifiable data may be provided to supervisors, faculty, or student affairs personnel to help ensure or verify compliance with other health and safety protocols enacted by the University.

As described by the University's Acceptable Use Policy, individually identifiable data may also be disclosed:

"In disciplinary proceedings, the University, at its discretion, may submit results of investigative actions to authorized University personnel or law enforcement agencies. Suspect communications created with University information technology resources may also be subject to Rhode Island's Public Records Statutes to the same extent as hardcopy communications. In addition, users may be subject to legally binding demands such as subpoenas and search warrants. Ultimately, it is the University that owns University IT resources, not employees who use them."

(ii) De-Identified Data

De-identified individual data as well as aggregated data may be used throughout the University and may be used for a variety of purposes. Among immediate potential uses under this policy are identification and resolution of group gatherings that exceed health limits, assessment of compliance with health attestations, monitoring of traffic patterns on URI property, and similar processes. In all situations, no individually identifiable characteristics will be preserved in the data.

When using de-identified data, the University will take reasonable efforts to ensure that re-identification is not possible. These efforts will include, but are not limited to, aggregating the de-identified data prior to use and/or sharing, and setting minimum cell size for reporting.

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
01.106.1	July 2, 2020	n/a	n/a
01.106.2	December 14, 2021	Scheduled Review	Removal of information regarding 2020-21 mandatory student testing; added information relative to vaccination information.