HIPAA AT URI: INTRODUCTION TO HIPAA and AN OVERVIEW OF HIPAA IMPLEMENTATION AT THE UNIVERSITY OF RHODE ISLAND

I. Background Information

The University of Rhode Island ("URI") has developed the attached set of policies and procedures, and standard forms, to comply with and implement the health information privacy and security related standards applicable to it under Title II, Subtitle F (entitled "Administrative Simplification") of the Health Insurance Portability and Accountability Act of 1996, or "HIPAA," as it was amended by the law known as the "HITECH Act" of 2009, and which is codified at 42 USC 1320d et. seq. (hereinafter the "HIPAA Statute"), and its applicable implementing regulations promulgated by the U.S. Department of Health of Human Services and appearing at 45 C.F.R. Parts 160, 162, and 164 (hereinafter the "HIPAA Regulations"), which include "The HIPAA Privacy Rule" (45 CFR Part 164, Subpart E), "The HIPAA Security Rule" (45 CFR Part 164, Subpart C), "The HIPAA Breach Notification Rule" (45 CFR Part 164, Subpart D) and other "general" and "administrative" requirements (e.g. general definitions) of the HIPAA Regulations.

II. General Requirements of HIPAA

A. HIPAA Applicability

The requirements of HIPAA apply to "covered entities" which the HIPAA regulations define as (a) "health plans," (b) "healthcare clearinghouses," and (c) "healthcare providers" who "transmit any health information in electronic form" in connection with certain types of "transactions" enumerated in the HIPAA Regulations (usually referred to as "covered transactions"), such as an electronic health insurance claim submission.

HIPAA also provides that an organization, like URI, "whose business activities include both covered functions and non-covered functions" ---- that is an organization which operates some units that perform functions that fall within the HIPAA definitions of "covered functions" (i.e. "health plan" functions; "health care clearinghouse" functions; "healthcare provider" functions) but that also operate other units that are outside of the - HIPAA definitions of "covered functions" (e.g. any academic or business unit that performs no functions related to health care) --- will be considered a "Hybrid Entity," and the requirements of HIPAA will only apply to those "components" (hereinafter "covered components") of the entity that actually perform "covered functions" as a HIPAA covered health plan, health care clearinghouse or health care provider.

Furthermore, HIPAA only applies to information defined in the HIPAA regulations as "protected health information" ("PHI"), which is "health information" (information that "relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present or future payment for the provision of health care to an individual") that "identifies the individual" or (it can reasonably be believed) "can be used to identify the individual," and does not fall into one of the HIPAA coverage exceptions for: health information

about an individual who has been dead for more than 50 years; employment records "held by a covered entity in its role as an employer"; information in "education records" covered by the federal law known as "FERPA"; and "treatment records" pertaining to students, who are 18 years of age or older, attending a postsecondary educational institution. Those last two "student" related exceptions, and their implementation at URI (i.e. their applicability to health care information relating to URI students) are discussed in more detail in Section III below.

Finally, the requirements of HIPAA will also apply to most vendors, contractors or other third parties with whom a covered entity shares PHI in order for that third party to perform some service for the covered entity. These third parties are referred to as "business associates" and HIPAA requires that they enter into a standard "business associate agreement" (containing certain required terms and conditions) with the covered entity, and become subject to the requirements of HIPAA in their own right.

B. HIPAA Preemption and Rhode Island State Law

There are a number of Rhode Island state laws and regulations that address the confidentiality of health information. The most prominent of them is the Rhode Island Confidentiality of Health Care Communication Act, RIGL, c. 5-37.3, ("RI-CHCCA") which establishes the basic privacy rules (including a general requirement of non-disclosure of "confidential health care information" without the individual's consent unless one of 24 exceptions applies) governing the use and disclosure of an individual's health information created or maintained a health care provider. Other relevant Rhode Island laws and regulations include those, for example, pertaining to medical records held by licensed physicians and medical practice groups.

The HIPAA statute and regulations make clear that, with a few limited exceptions, the provisions of HIPAA will "preempt" (i.e. have priority over, and effectively negate) state laws and regulations which are "contrary" to HIPAA (i.e. state laws which would, if adhered to, cause a non-compliance with a HIPAA regulation). However, the HIPAA Regulations also make clear that, in general, if a provision of state law that "relates to the privacy of individually identifiable health information" is "more stringent" than a HIPAA requirement, the stricter state law should be followed. A state law will be considered "more stringent," for example, when it prohibits a disclosure that HIPAA would allow, or when it provides the individual with broader rights (e.g. access rights) in their medical records than HIPAA does.

A careful comparison of the requirements of the HIPAA Regulations with the requirements of all relevant Rhode Island health information privacy and security laws and regulations was performed, and it revealed that HIPAA protections were either the same as, or stronger than, Rhode Island law in all but a few instances. In the few cases where Rhode Island law was "more stringent" – e.g. in providing fewer exceptions to a patient's ability to obtain access to their medical records – the stricter Rhode Island provision was included in the attached URI policies. In short, the attached URI HIPAA policies are considered to be fully compliant with both HIPAA and the relevant (non-conflicting) requirements of Rhode Island state law.

C. The HIPAA Privacy Rule

The HIPAA Privacy Rule generally governs the permitted and prohibited uses and disclosures of health information by "covered entities," and establishes the access

and other rights individuals have in their health information which is held by covered entities. The Privacy Rule is long and fairly complex, and while no attempt will be made here to describe its requirements in significant detail, its main provisions can be very briefly summarized as follows: The Privacy Rule establishes requirements and standards relating to: (1) When, and under what conditions, PHI may be used or disclosed by a covered entity without the written authorization of the individual (e.g. for "treatment, payment or health care operations"; for required reporting of communicable disease information to public health agencies; to respond to a court order or lawful subpoena); (2) When and under what conditions, PHI may be used or disclosed by a covered entity after the individual is given notice and opportunity to object to the use or disclosure (e.g. disclosures to family members or friends who will have involvement in care related decisions or communications); (3) the required content of written authorization forms; (4) the posting and distribution of the entity's standard "notice of privacy practices" and the required contents of such notice; (5) the right of patients to request amendments of their medical records, and the rules for making, and documenting in the medical record, both "accepted" amendments, and proposed amendments not accepted by the covered entity; (6) the circumstances in which PHI may be used and disclosed for purposes of "research" and the conditions and limitations pertaining to research related uses and disclosures; (7) accepted methods for "de-identifying" PHI; (8) how to document, and make available upon the individual's request, an "accounting" of disclosures of the individual's PHI made by the covered entity; and (9) other various "administrative requirements" covered entities must comply with (e.g. maintaining required HIPAA policies and procedures, including sanctions and non-retaliation policies, and updating them when necessary to reflect changes in the law; a minimum 6 years record retention period; employee training; complaint processes; mitigating harm from known regulatory violations; and designation of an institutional HIPAA privacy official).

D. The HIPAA Security Rule

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI. Specifically, covered entities must take appropriate steps to (1) maintain the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; (2) identify and protect against reasonably anticipated threats to the security or integrity of the information; (3) protect against reasonably anticipated, impermissible uses or disclosures; and (4) ensure compliance by their workforce. The Security Rule is flexible and "scalable" in that it allows covered entities to analyze their own needs and implement solutions appropriate for their specific environments. The first step in achieving compliance is for the covered entity to perform a "risk assessment" for each of its covered components, which will guide the identification and implementation of the appropriate security safeguards needed to protect against those risks. The Security Rule also establishes 18 "standards" as well as "required" and "addressable" "implementation specifications" for each of them. Covered entities must establish appropriate policies, procedures and practices that meet all required and addressable specifications in the rule, although they have the flexibility to establish a reasonable "alternative method" of complying with "addressable" specifications, provided they properly document the alternative method and the reasons why it is considered reasonable.

E. The HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, DHHS, and in some cases the media, of a breach of unsecured PHI. Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to DHHS annually. The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate. The notification requirements can be avoided in cases where the covered entity reasonably determines that there was a "low probability" that PHI was actually compromised.

F. Other HIPAA Administrative Requirements and Enforcement Provisions

The HIPAA Regulations (in 45 CFR Part 164, Subpart A) also require that covered entities who are hybrid entities (like URI) designate, and document the designation of, its "healthcare components" which are commonly also referred to (and are referred to in the attached URI HIPAA Policies and Procedures simply) as "covered components." The HIPAA Regulations rules also make clear that the hybrid entity must include within each "covered component," not only the unit that functions as a health care provider (or health plan or health care clearinghouse), but also the other units in the organization (such as the institution's legal office) that from time to time will need to receive PHI from that unit in order to assist that unit in meeting its legal, administrative, or business obligations. These units, which are sometimes referred to informally "internal business associate" units, must be listed in the covered entity's description of the covered component, and must also use or adhere to all applicable HIPAA regulations with respect to the PHI they receive and maintain. The HIPAA Regulations also make clear that the organization itself (the hybrid entity) maintains overall responsibility for regulatory compliance, including ensuring that each of its covered components remains in compliance.

Finally, the administrative "enforcement" and "adjudicatory" provisions of HIPAA (e.g. the procedures and rules relating to DHHS investigations, enforcement actions, hearings, decisions, appeals, and the imposition of civil administrative penalties) are set forth in 45 CFR Part 160 (entitled "General Administrative Requirements"). It should be noted that, in addition to seeking civil monetary penalties (which may be as high as $50,000.00 per violation, and even more in serious cases involving willful neglect and failure to timely correct), the federal government may in some extreme cases (e.g. those involving the sale of PHI) bring criminal complaints and seek fines of as high as $250,000 per violation, and imprisonment of up to 10 years, although such prosecutions appear to be extremely rare.

III. Applicability of HIPAA Regulations to URI

A. URI Designation as a "Hybrid Entity" Under HIPAA

Based on a comprehensive assessment of URI's departments, programs and activities conducted in 2017 by a designated HIPAA Compliance Initiative Working Group, and which included the completion of a "HIPAA Inventory Survey" by URI officials whose departments and programs were understood to have some involvement in the provision of health related services, it was determined that four (4) university units performed "covered functions" as "health care providers" and were subject to HIPAA requirements

because they conducted some "covered transactions (e.g. health insurance billing) electronically. Those "URI Covered Health Care Components" are described in the following section. As a result, the University is required to designate itself, and has designated itself, as a "Hybrid Entity" (i.e. an entity that performs both HIPAA-covered functions and non-HIPAA-covered functions) for purposes of HIPAA.

B. HIPAA Applicability to URI Covered Health Care Components

The following URI units were determined to be "covered health care components" under HIPAA by virtue of their (a) functioning as "health care providers" as defined by HIPAA, (b) "transmit[ting] health information in electronic form" in connection with HIPAA "covered transactions" such as health insurance billing or receipt of payment, and (c) providing services to, and maintaining the PHI of, individuals who are not URI students [**Note**: Since HIPAA does not apply to health information about URI students held by URI (as further discussed in subsections II(A) above and III(C) below), URI units that would otherwise be considered "covered health care components," but that provide services ONLY to URI students --- such as the URI Athletic Department (which provides and bills insurers electronically for "athletic trainer" type health care services it provides) --- are not considered to be subject to HIPAA and will not be listed here, or treated as, "covered health care components" for purposes of HIPAA. The covered healthcare providers identified by URI, and listed below, provide services **to at least some individuals who are not URI students**, although they may in addition provide services to URI students as well.]

1. URI Health Services
2. URI Emergency Medical Services
3. University Physical Therapy
4. URI Speech and Hearing Centers

Because each of the above-listed URI "covered health care components" may, from time to time, need to disclose PHI about their patients/clients to The URI Office of General Counsel, the URI Office of Information Technology Services, and the URI Office of the Chief Information Security Officer, in order for them to obtain and utilize the assistance of those offices in meeting their business, legal, administrative, business and technology related obligations, those offices will be listed as an integral part of each of the four "covered health care components," and functionally treated as their "internal business associates," as required by HIPAA.

The above listed covered health care components shall comply with all applicable HIPAA Regulations and all of the URI HIPAA policies and procedures.

C. HIPAA Applicability to URI "Business Associate Components"

Because HIPAA obligations also extend to "business associates" of covered entities (i.e. persons or organizations who perform services for the covered entity which require the use of the covered entity's PHI), URI evaluated its operations to determine whether any department, office, unit or employee of URI functioned as a "business associate" of any outside covered entity. As a result of that evaluation, it was determined that the following URI units function as "business associates" of third parties who are HIPAA covered entities:

1. The DataSpark Program within the URI Libraries
2. The Department of Pharmacy Practice within the URI College of Pharmacy

Accordingly, the above listed units shall be considered and referred to as "URI Business Associate Components" and shall be subject to the HIPAA Regulations, and the attached URI HIPAA policies, in the same way as URI Health Care Components. These units shall also be subject to all of the terms and conditions of the required "Business Associate Agreement" URI enters into on behalf (in the exclusive discretion of URI) with the external HIPAA covered entities for whom they perform services.

D. HIPAA Applicability Exception for Health Information About URI Students: HIPAA Does Not Apply to URI Student Health Information

The attached HIPAA policies apply to all PHI held by URI Covered Components that relate to individuals other than URI students; In other words, the attached HIPAA policies do not apply to health care information pertaining to URI students.

Rather, personally identifiable Health Care Information ("HCI") pertaining to URI students that is held by any URI unit (whether a HIPAA "Covered Component" or not) will need to be maintained, used and disclosed by that URI unit: (1) in compliance with the applicable provisions of Rhode Island Law (primarily the Rhode Island Confidentiality of Health Care Communication Act, RIGL, c. 5-37.3 available at http://webserver.rilin.state.ri.us/Statutes/TITLE5/5-37.3/INDEX.HTM) when the HCI is included in a "treatment record;" and (2) in compliance with both the applicable provisions of Rhode Island Law (primarily the Rhode Island Confidentiality of Health Care Communication Act, RIGL, c. 5-37.3 available at http://webserver.rilin.state.ri.us/Statutes/TITLE5/5-37.3/INDEX.HTM) AND the federal education record privacy law known as "FERPA" (the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, and the law's implementing regulations, 34 C.F.R. Part 99, available at https://www2.ed.gov/policy/gen/reg/ferpa/index.html) and described and summarized in URI Guidance (at https://web.uri.edu/enrollment/ferpa/) when the HCI is included in an "education record."

"Treatment Records" are records held by any URI unit which are (i) made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity; (ii) made, maintained, or used only in connection with treatment of the student; and (iii) disclosed only to individuals providing the treatment.

"Education Records" are all records pertaining to the student maintained by the unit other than "treatment records." It is important to note, however, that a "treatment

record" will become an "education record" once it is disclosed to the student, or to any third person

E. No URI Health Plans or Healthcare Clearinghouses

Because the State of Rhode Island, and not URI itself, sponsors and/or operates all "health plans" (as that term is defined in the HIPAA Regulations) available to URI employees, it has been determined that URI has no "health plan" related compliance obligations under HIPAA.

Furthermore, because it has also been determined that neither URI, not any unit of URI, functions as a "health care clearinghouse" under HIPAA, URI has no "health care clearinghouse related compliance obligations under HIPAA

F. HIPAA Implementation Steps at URI

To meet its obligations under HIPAA, the following steps will be undertaken, or commenced, immediately upon official adoption of the attached URI HIPAA Policies by URI, which will occur upon the approval (i.e. by a written approval memo) of the URI President, which is expected to occur in January 2018:

1. The URI HIPAA Policies will be posted on an appropriate public-facing webpage of the URI website.
2. The adoption of the policies will be announced to the URI community, through a written campus wide communication which will include a link to the online policies.
3. Training and education concerning the URI HIPAA Polices will promptly be provided to all appropriate employees of the URI Covered Health Care Components and the URI Business Associate Components (collectively "URI Covered Components").
4. All elements of the URI HIPAA policies shall take effect immediately upon adoption. Each URI Covered Component shall be expected to fully comply with all requirements of the URI HIPAA policies within 60 days of their adoption, provided however, that compliance with all aspects of the HIPAA Security Rule (and URI HIPAA Policies 40 through 43, which relate to Security Rule compliance) shall occur as soon as possible, following the performance of risk assessments and the compliance action steps outlined in the following section.
5. In furtherance of ensuring full compliance with the HIPAA Security Rule (and URI HIPAA Policies 40 through 43, which relate to Security Rule compliance), the URI HIPAA Security Officer will commence immediately to perform individual "risk assessments" for each URI Covered Component, following which appropriate and documented health information security policies, procedures and practices will be established (informed by the component's individualized risk assessment) for each URI Covered Component which address and satisfy each of the HIPAA Rule standards, and required and addressable implementation specifications. This will be performed, on an expedited basis, with compliance expected as soon as possible.
6. Assurance of ongoing compliance by URI with HIPAA and the URI HIPAA Policies will be the joint responsibility of the URI HIPAA Privacy Officer, the URI HIPAA Security Officer, and the HIPAA Compliance Oversight Committee, as described in the following Section III(G).

G. 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: Patricia Parkes
   Coordinator, Health Information Management
   URI Health Services

2. URI HIPAA Security Officer: Michael Khalfayan,
   Associate Director, Information Security
   URI Information Technology Services

In serving in those roles, the above-named individuals will carry out all of the required responsibilities for their roles, as described in the HIPAA Regulations and the attached URI HIPAA policies

Finally, the University has established a HIPAA Compliance Oversight Committee which has been charged with the following general responsibilities: helping implement the URI HIPAA policies and procedures following their initial adoption; participating in required employee training and education; assisting URI's HIPAA-covered health care components and business associate components addressing issues and questions related to HIPAA implementation and compliance; leading the University's responses to relevant changes in the law (e.g. amendments to the HIPAA Regulations), or relevant changes in University operations (such as offering a new HIPAA covered health service); periodically assessing HIPAA compliance at the University, and issuing findings and recommendations based on those assessments when needed; and helping respond to security breaches and instances of non-compliance. The Committee shall include, at a minimum, the following members:

- HIPAA Privacy Officer (Patricia Parkes)
- HIPAA Security Officer (Michael Khalfayan)
- Lead HIPAA Counsel (Peter Harrington)
- Designated Human Resources representative ( )
- Designated "Covered Component" ("stakeholder") representative ( )
- Director of URI Health Services (Ellen Reynolds)
- URI Chief Information Officer ( )

The HIPAA Compliance Oversight Committee will be co-chaired by the Lead HIPAA Counsel (Peter Harrington) and the Director of URI Health Services (Ellen Reynolds), and shall meet whenever necessary, and at least annually.