Executive Policy Chapter 2, Administration
Executive Policy EP 2.217, HIPAA Policy
Effective Date: June 2017
Prior Dates Amended: None
Responsible Office: Office of the Vice President for Information Technology & Chief Information Officer
Governing Board of Regents Policy RP 2.202 – Duties of the President
Review Date: May 2020

## I. Purpose

The purpose of this executive policy is to ensure that the University of Hawai'i (the "University") complies with the Health Insurance Portability and Accountability Act of 1996, as amended by the American Recovery and Reinvestment Act of 2009 ("ARRA"), which included the Health Information Technology for Economic and Clinical Health Act ("HITECH") that expanded the scope of privacy and security protections, and by the implementing regulations at 45 Code of Federal Regulations ("CFR") Parts 160, 162 and 164, as amended (collectively referred to as "HIPAA"). The objectives of this policy (hereinafter, "HIPAA Policy") are to establish University System-wide policies and procedures to:

A. Designate the University as a Hybrid Entity as defined in HIPAA.
B. Establish fundamental principles governing the University's management and use of Protected Health Information ("PHI") as required by HIPAA, including electronic Protected Health Information ("ePHI") as all such terms are defined in HIPAA and as more specifically set forth in paragraphs II.H and T herein.
C. Establish a set of standardized terms and definitions to promote consistent interpretation and implementation of the University's HIPAA Policy.
D. Establish clear lines of authority and accountability related to PHI.
E. Set forth best practices for HIPAA compliance with the ongoing objectives of:
    1. Identifying University units and subunits (and their activities) that are subject to HIPAA (collectively the "UH Covered Components") that are more specifically defined in this HIPAA Policy in paragraphs II.V and III.A.
    2. Managing and mitigating information privacy and security risks related to PHI.

The federal regulations protecting PHI are complex, and this University HIPAA Policy distills those regulations and provides for additional training regarding the regulations. An annotated version of the Policy, which contains citations to specific regulations, is available from the University System HIPAA Privacy and Security Officer(s) (defined herein and as more specifically set forth in paragraph III.E herein). In

the event of any inconsistency between this HIPAA Policy and HIPAA, HIPAA shall control. Any questions about this HIPAA Policy may be directed to the "Unit HIPAA Coordinator" and the "UH System HIPAA Privacy and Security Officer(s)" (as defined herein), or the Chief Information Security Officer or the Office of General Counsel, as appropriate.

This HIPAA Policy covers PHI, which does not include all health information collected by the University. PHI does not include, for example, information that is considered education records covered by the Family Educational Right and Privacy Act ("FERPA") and excluded from HIPAA, as well as employment records held by any unit or subunit in its role as an employer. Any health information not protected under this HIPAA Policy is covered under Executive Policy ("EP") 2.214, as amended, and other applicable University policies, and all University units and subunits maintaining such non-PHI health information must comply with EP 2.214.

## II. Definitions

The University adopts and uses the following definitions set forth in HIPAA, specifically including the HIPAA regulations at 45 CFR Parts 160, 162, and 164, as amended. Capitalized terms are used herein as defined in HIPAA unless the context requires otherwise.

A. Authorization: A document that is required to be signed by the patient to use and disclose specified PHI for specified purposes. (A standard University Authorization template is attached hereto as Attachment 1-A.)

B. Business Associate: A person or entity (other than an employee of a UH Covered Component) who performs a function or activity involving the use or disclosure of PHI on behalf of a Covered Entity, including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, re-pricing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Business associates include a health information organization, e-prescribing gateway, or other vendors who provide data transmission services that require access to PHI on a routine basis; entities that offer personal health records; and subcontractors that receive PHI on behalf of the business associate. A business associate of one UH Covered Component does not automatically become a business associate of any other UH Covered Component.

C. Consent: A general document that Covered Entities may obtain giving health care providers, which have a direct treatment relationship with a patient, permission to use and disclose all PHI to carry out treatment, payment or health care operations. It gives permission only to that provider, not to any other person. Health care providers may condition the provision of treatment

on the individual providing this consent. One Consent may cover all uses and disclosures for treatment, payment or health care operations by that provider and business associates, indefinitely. A Consent need not specify the particular information to be used or disclosed, nor the recipients of disclosed information. (A standard University Consent template is attached hereto as Attachment 1-B.)

D. Covered Entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form.

E. Covered Function: Those functions of a Covered Entity, the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

F. Direct Treatment Relationship: A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

G. Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside of the entity holding and/or maintaining the information.

H. Electronic Protected Health Information ("ePHI"): Information that is transmitted or maintained by electronic media that comes within the definition of PHI as defined below.

I. Health Care Component: A component of a Hybrid Entity designated by the Hybrid Entity that functions as a health care provider, as defined by HIPAA.

J. Health Care Operations: Any of the activities set forth in the HIPAA regulations that includes but is not limited to the following:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs; protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating performance, conducting training programs for health care and non-health care professionals, and participating in accreditation, certification, licensing or credentialing activities;
3. Underwriting, premium rating and other activities relating to health plan contracts;
4. Conducting medical review, legal services, auditing and compliance functions;
5. Business planning and development and business management and general administrative activities, including, but not limited to, customer service, resolution of internal grievances, and due diligence.

K. HIPAA Privacy Rule: The HIPAA Privacy Rule is defined as set forth in 45 CFR Part 160 and Subparts A and E of Part 164.

L. HIPAA Security Rule: The HIPAA Security Rule is defined as set forth in 45 CFR Part 160 and Subparts A and C of Part 164.

M. Hybrid Entity: A single legal entity that is a Covered Entity whose business activities include both Covered Functions and non-Covered Functions.

N. Indirect Treatment Relationship: A relationship between an individual and a health care component in which the health care component delivers health care to the individual based on the orders of another health care provider and the health care component typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the patient.

O. Individual: The person who is the subject of PHI.

P. Individually Identifiable Health Information ("IIHI"): Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) 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; and (3) That identifies the individual, or might reasonably be used to identify the individual.

Q. Minimum Necessary: To make reasonable efforts to limit the use or disclosure of, and requests for, PHI to the least amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

R. Payment: The activities described in HIPAA, including, but not limited to, those undertaken by a provider to obtain or provide reimbursement for the provision of health care, including, but not limited to determinations of eligibility or coverage; risk adjusting amounts due; billing, claims management, and collection activities; review of health care services with respect to medical necessity and coverage; utilization review activities, including precertification and preauthorization of services; and disclosure to consumer reporting agencies of the following information: name/address, date of birth, social security number, payment history, account number, and name and address of the provider.

S. Personal Representative: Someone with the legal authority to act on behalf of an incompetent adult patient, a minor patient or a deceased patient or the patient's estate in making health care decisions or in exercising the patient's rights related to the individual's PHI.

T. Protected Health Information ("PHI"): Health information, including demographic information collected from an individual and created or received by a health provider, health plan, employer, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any 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, and that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium. (PHI does not include IIHI in education records covered by FERPA and excluded from HIPAA, as well as employment records held by any unit or subunit in its role as an employer.)

U. Treatment: The provision, coordination, or management of health care services by providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for health care from one provider to another.

V. UH Covered Components: Units or subunits of the University designated by the University as Covered Entities and required to comply with HIPAA because the unit or subunit performs a Covered Function as a health care component. (The terms "UH Covered Component" or "UH Covered Components" are distinguishable from the generic HIPAA term "Covered Entity" defined above.)

W. Use: The sharing, employment, application, utilization, examination or analysis of PHI within an entity that maintains the PHI.

X. Workforce: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a UH Covered Component or Business Associate, is under the direct control of such UH Covered Component or Business Associate, whether or not they are paid by the UH Covered Component, the University, or Business Associate.

## III. Executive Policy

### A. Policy Statement and Designation of UH Covered Components

The University is Hawai'i's statewide higher education system and only public university. The University is a body corporate as provided in Article X, Section 5 of the Hawai'i State Constitution. Pursuant to that authority and as allowed by HIPAA, the University designates itself as a Hybrid Entity separate from the State of Hawai'i Executive, Legislative and Judicial branches.

The University is committed to complying with HIPAA. The University is a single legal entity comprised of separate campuses, schools, departments, entities,

units and subunits (collectively referred to as "Units"). Some Units provide Covered Functions as defined in HIPAA and have been designated by the University as "UH Covered Components" and other Units perform non-covered functions under HIPAA. Accordingly, the University has designated itself as a Hybrid Entity in accordance with the applicable HIPAA regulations. A Hybrid Entity may exclude from its Covered Entity status the following non-covered functions: (1) non-health care components of the organization, e.g., the University's academic programs, and/or (2) health care components of the organization that do not engage in electronic transactions, e.g., a clinic that provides health care services but does not bill for its services. All UH Covered Components must comply with HIPAA. Furthermore, to the extent that any University Unit is required to enter into a BAA and/or Subcontractor Agreement, as defined in HIPAA, such Unit will also be subject to HIPAA and designated as a UH Covered Component. The University may also designate other University Units as UH Covered Components to the extent that they perform a function and provide services for a designated UH Covered Component, but are not themselves providing treatment, payment or health care operations, and are designated as Business Associates of a designated UH Covered Component.

University Units that are designated as UH Covered Components are listed on the University's HIPAA Policy website: http://www.hawaii.edu/infosec/hipaa

University Units that collect, use, transmit, and/or store IIHI but are not designated as UH Covered Components are still required to: (1) protect IIHI in accordance with applicable HIPAA privacy and security policies and (2) comply with the operational procedures set forth herein.

## B. General Requirements and Practices

1. The designated UH Covered Component may not share PHI with the non-covered Units of the University unless specifically allowed by HIPAA and this HIPAA Policy. Each UH Covered Component shall comply with HIPAA and require its employees, students, volunteers, consultants, and contractors to comply with HIPAA and this HIPAA Policy. A UH Covered Component may not modify or delete any portion of this HIPAA Policy.
2. Each UH Covered Component has performed a risk assessment as required by HIPAA that shows compliance with HIPAA and this HIPAA Policy.
3. Each UH Covered Component must designate a Unit HIPAA Coordinator to assist the UH System HIPAA Privacy and Security Officer(s) in carrying out this HIPAA Policy and all University policies and procedures related to the privacy and security of PHI and ePHI under HIPAA.

4. The appropriate Unit employees, students and volunteers of each designated UH Covered Component have satisfactorily completed training required by HIPAA and any updates to training as required by HIPAA.
5. Each UH Covered Component has a BAA with another internal University Unit or an entity outside the University to share PHI or a Limited Data Set.
6. Each UH Covered Component that provides a Limited Data Set pursuant to HIPAA to another University Unit or an entity outside the University has a current Data Use Agreement and BAA with such University Unit or outside entity that receives the Limited Data Set, and such use has been approved by the University's Institutional Review Board ("IRB").
7. Each UH Covered Component provides and posts a Notice of Privacy Practices as required by HIPAA. (A standard University Notice of Privacy Practices template is attached hereto as Attachment 2.)

C. **Privacy Policies and Procedures**

1. Disclosure only with consent. A UH Covered Component may not use or disclose PHI without the consent of the individual, except disclosures for treatment, payment, or health care operations, and for certain incidental or limited uses in compliance with HIPAA. 45 CFR § 164.502 and 164.506.
2. Disclosure required to individual and DHHS. A UH Covered Component is required to disclose PHI to an individual when requested (45 CFR § 164.524 or §164.528) and when required by the Secretary of the Department of Health and Human Services ("DHHS") to investigate or determine the UH Covered Component's compliance with HIPAA.
3. Disclosure to UH Covered Component. When using or disclosing PHI or when requesting PHI from another UH Covered Component, the UH Covered Component must make reasonable efforts to limit PHI use or disclosure to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request except as otherwise provided by HIPAA.
4. Disclosure to Business Associate. A UH Covered Component may disclose PHI to a business associate and may allow a business associate to create, receive, maintain, or transmit PHI on its behalf, if the UH Covered Component obtains assurances that the business associate will appropriately safeguard the information. Such assurances must be documented through a BAA that complies with HIPAA. (Standard University BAAs are attached hereto as Attachments 3-A (Unit is the Covered Entity) and 3-B (Unit is the Business Associate).)
5. Disclosure pursuant to valid authorization. When a UH Covered Component obtains or receives a valid authorization, use and disclosure of any PHI under such authorization must be consistent with such

authorization.

6. Disclosure for marketing purposes. The UH Covered Component must obtain authorization for any use or disclosure of PHI for "marketing" purposes, unless it is face-to-face communication between the UH Covered Component and the individual, or a promotional gift of nominal value provided by the UH Covered Component. Marketing is communication about a product or service which encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
    a. to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if the financial remuneration received by the UH Covered Component in exchange for making the communication is reasonable in relation to the UH Covered Component's costs of making the communication; or
    b. for the following purposes except where the UH Covered Component receives financial remuneration in exchange for the communication:
        1) to describe a health–related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication (including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits);
        2) for treatment of the individual, including case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; or
        3) for case management or care coordination, contacting of individuals with information about treatment alternatives and related functions to the extent that these activities do not fall within the definition of treatment.
7. Disclosure of psychotherapy notes. The UH Covered Component must obtain prior written authorization from the patient for any disclosure of psychotherapy notes for any reason (with limited exceptions).
    a. Psychotherapy notes are notes recorded by a provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication

prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date

b. The UH Covered Component should always consult the applicable regulations for specific guidance on protecting psychotherapy notes. Any questions about compliance should be directed to the UH Covered Component's Unit HIPAA Coordinator, or the UH System HIPAA Privacy and Security Officer(s).

8. Disclosure relating to minors. While HIPAA uses the terms "emancipated minor" and "unemancipated minor," HIPAA defers to state law regarding the disclosure of PHI relating to a minor. Accordingly, this paragraph III.C.8 is based on HIPAA and applicable State law. The UH Covered Component should always consult the applicable laws and regulations for specific guidance on disclosure relating to minors. Any questions about compliance should be directed to the UH Covered Component's Unit HIPAA Coordinator, or the UH System HIPAA Privacy and Security Officer(s).

   a. *Relevant definitions*.
      1) For purposes of this policy, a "minor" is generally any person under the age of 18.
      2) "Emancipated Minor" is a minor (under 18) who is to be treated as an adult for purposes of this policy. Under this policy, an emancipated minor is
      (1) a minor who has been married and is thus considered to have reached the age of majority (18); or
      (2) a minor who is totally self-supporting.
      (This definition of Emancipated Minor incorporates both HIPAA and applicable state law.)
      3) "Personal Representative" is a person with authority to act for the Emancipated Minor in making decisions related to health care. A Personal Representative has the same powers as the Emancipated Minor to the extent allowed under applicable state law.
      4) A "minor without support," is a person who is at least 14 but less than 18 years of age, who is not under the care, supervision, or control of a parent, custodian or legal guardian. Minors without support may consent to primary medical treatment and services under certain circumstances. A minor without support who receives services is deemed to have legal capacity to consent to such treatment and such consent is binding as if the minor without support reached the age of majority. Because these provisions deem a minor without support to have reached the age of majority,

such a minor qualifies under HIPAA as the only person who can sign an Authorization for release of PHI.

5) An "unemancipated minor" is a person under 18 years of age who is not an Emancipated Minor as defined above.

b. *Disclosure to a minor's parent, guardian, or person acting in lieu of a parent, i.e., Personal Representative, and Authorization by Personal Representative.*

1) A licensed health care professional may release PHI to a parent, guardian or person acting in lieu of a parent if (a) such release is allowed by state law and (b) approved by a licensed health care professional, in the exercise of professional judgment. *See* 45 CFR 164.502(g)(3)(ii)(A)-(C).

2) In situations where the parent, guardian or person acting in lieu of a parent *of* an unemancipated minor has the authority to act on behalf of the minor as the minor's Personal Representative, and an Authorization to use or disclose the minor's PHI is required, the Authorization may be signed by the minor's Personal Representative.

c. *Disclosure requiring Authorization by the minor.* If the minor has the authority to act on his/her own behalf in receiving health care services, e.g., an Emancipated Minor or a "minor without support", then the minor must sign his/her own Authorization and must authorize disclosure of the minor's PHI.

d. *Disclosure (at the discretion of treating physician) requiring consultation with the minor (ages 14 – 17).*

1) Public and private hospitals, or public and private clinics or physicians licensed to practice medicine, *at the discretion of the treating physician* (excluding other care providers who are not physicians, e.g., psychologists, advanced practice nurses, etc.), may inform the spouse, parent, custodian, or guardian of any minor patient (ages 14 – 17) of the provision of medical care and services (including the diagnosis, examination, and administration of medication in the treatment of *venereal diseases, pregnancy, and family planning services*, but excluding surgery or any treatment to induce abortion) to such minor patient or disclose any information pertaining to such care and services *after consulting with such minor patient* to whom such medical care and services have been provided. If the minor patient is not diagnosed as being pregnant or afflicted with venereal disease, the treating physician may disclose such information as well as the application for diagnosis, at the discretion of the treating physician after consulting with such minor patient.

2) Written authorization is not required for such a disclosure since only consultation is required. If the minor (ages 14 – 17) is diagnosed as

pregnant or afflicted with venereal disease, the treating physician probably cannot disclose such information to the parents or guardians without permission from such minor

9. Disclosure requiring advance notice and opportunity to agree or object. A UH Covered Component may use or disclose PHI, provided that the individual is informed in advance and has the opportunity to agree to or prohibit or restrict the use or disclosure in accordance with applicable HIPAA regulations (*see* 45 CFR § 164.510). The UH Covered Component may verbally inform the individual of and obtain the individual's verbal agreement or objection to a use or disclosure permitted by the HIPAA regulations. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the UH Covered Component may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the individual's care or payment or that is needed for notification purposes. A UH Covered Component may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing another person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

10. Disclosure when authorization or opportunity to agree or object not required.

    a. A UH Covered Component may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
    b. A UH Covered Component may use or disclose PHI for the public health activities and purposes as provided in relevant HIPAA regulations (*see* 45 CFR § 164.512).
    c. A UH Covered Component may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight.
    d. A UH Covered Component may disclose PHI in the course of any judicial or administrative proceeding: (1) in response to an order of a court or administrative tribunal, provided that only the PHI expressly authorized is disclosed, or (2) in response to a subpoena, discovery request or other lawful process.
    e. A UH Covered Component may disclose PHI for a law enforcement purpose to a law enforcement official if: (1) required by law or (2) in

compliance with court proceedings or administrative requests if information sought is relevant to a legitimate law enforcement inquiry, and de-identified information could not reasonably be used.

11. Disclosure to determine identity or cause of death. A UH Covered Component may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

12. Disclosure for research purposes. A UH Covered Component may use or disclose PHI for research, regardless of the source of funding of the research, provided that:

    a. The UH Covered Component obtains documentation that an alteration to or waiver of the individual authorization for use or disclosure of PHI has been approved by a University IRB.
    b. The UH Covered Component obtains from the researcher representations that use or disclosure is solely to review PHI to prepare or advance research, and no PHI is removed from the UH Covered Component.
    c. A brief description of the PHI has been deemed to be necessary by the University IRB.
    d. A statement that the alteration or waiver of authorization has been reviewed and approved, and signed by the chair or other member (designated by the chair) of the University IRB.

13. Disclosure to prevent/lessen imminent threat of harm. A UH Covered Component may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if it believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, or necessary to law enforcement authorities to identify or apprehend an individual.

14. Disclosure for workers compensation purposes. A UH Covered Component may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs that provide benefit for work-related injuries or illness.

15. Disclosure of de-identified data. Heath information is not IIHI if (1) it does not identify an individual; and (2) there is no reasonable basis to believe that the information can be used to identify an individual. Data which lack these elements are excluded from the HIPAA regulations governing PHI use. Such de-identified data must have the following identifiers removed:

    a. Names.
    b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to

the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
d. Telephone numbers;
e. Fax numbers;
f. Electronic mail addresses;
g. Social security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;
l. Vehicle identifiers and serial numbers, including license plate numbers;
m. Device identifiers and serial numbers;
n. Web Universal Resource Locators ("URLs");
o. Internet Protocol ("IP") address numbers;
p. Biometric identifiers, including finger and voice prints;
q. Full face photographic images and any comparable images; and
r. Any other unique identifying number, characteristic or code.

16. Disclosure of Limited Data Set. A UH Covered Component may use or disclose a Limited Data Set if the UH Covered Component enters into a Data Use Agreement with the Limited Data Set recipient and a BAA.

    a. A Limited Data Set is PHI that excludes the following direct identifiers:
        1) Names;
        2) Postal address information, other than town or city, State, and zip code;
        3) Telephone numbers;
        4) Fax numbers;
        5) Electronic mail addresses;
        6) Social security numbers;
        7) Medical record numbers;
        8) Health plan beneficiary numbers;
        9) Account numbers;
        10) Certificate/license numbers;
        11) Vehicle identifiers and serial numbers, including license plate numbers;
        12) Device identifiers and serial numbers;

13) Web URLs;
14) IP address numbers;
15) Biometric identifiers, including finger and voice prints; and
16) Full face photographic images and any comparable images.

b. A Limited Data Set may only be disclosed for the purposes of research, public health or health care operations.
c. A Data Use Agreement pursuant to this section must meet the requirements of 45 CFR § 164.514(e) and be approved by the University IRB.

17. Disclosure consent requires prior notice of privacy practices. An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the UH Covered Component, and of the individual's rights and the UH Covered Component's legal duties with respect to PHI (exceptions include group health plans and inmates).

a. The UH Covered Component must provide a notice that is written in plain language and that contains the following required elements:
   1) The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
   2) Uses and disclosures;
   3) Separate statements for certain uses or disclosures;
   4) Individual rights;
   5) UH Covered Component's duties;
   6) Complaints;
   7) Contact; and
   8) Effective date.

b. A UH Covered Component must revise and distribute its notice whenever there is a material change to the uses or disclosures, individual's rights, the UH Covered Component's legal duties, or other privacy practices as required by law.
c. A UH Covered Component must make the required notice available on request to any person and to individuals as specified.
d. Requirements for electronic notice: A UH Covered Component that maintains a website must make the notice prominently available on its website. A UH Covered Component may provide notice via email if the individual has agreed to such notice and other requirements of this section are met.

e. A UH Covered Component must document compliance with the notice requirements, by retaining copies of the notices issued by the UH Covered Component and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement.

f. A standard University Notice of Privacy Practices template is attached hereto as Attachment 2.

18. Disclosure by Unit which is a federally assisted drug abuse program or a federally assisted alcohol abuse program.

a. Generally, with certain limited exceptions, the written consent of the individual is required before PHI identifying a patient as an alcohol or drug abuser either directly, by reference to other publicly available information, or through verification of such an identification by another person, before such PHI can be released to third parties. Examples of such exceptions may include but are not limited to:
(1) Veterans' Administration.
(2) Armed Forces.
(3) Communication within a program or between a program and an entity having direct administrative control over that program.
(4) Qualified Service Organizations. (42 CFR § 2.11)
(5) Crimes on program premises or against program personnel.
(6) Reports of suspected child abuse and neglect.

b. This paragraph III.C.18 is not part of HIPAA; rather, it is based on 42 CFR Part 2, *Confidentiality of Alcohol and Drug Abuse Patient Records*. 42 CFR Part 2. The UH Covered Component should always consult the applicable regulations for specific guidance on protecting drug and alcohol abuse records. Any questions about compliance should be directed to the UH Covered Component's Unit HIPAA Coordinator, or the UH System HIPAA Privacy and Security Officer(s).

19. Rights to request privacy protection for PHI. A UH Covered Component must permit an individual the right to request that the UH Covered Component restrict use or disclosure of PHI about the individual to carry out treatment, payment, or health care operations and restrictions related to family members, friends, and others listed in the HIPAA regulations.

a. A UH Covered Component is not required to agree to a restriction except as provided below in Paragraph III.C.19.e .

b. In general, if there is a restriction, the UH Covered Component may not use or disclose PHI in violation of such restriction, except in case of an emergency.

c. If restricted PHI is disclosed to a health care provider for emergency treatment, the UH Covered Component must request that such health care provider not further use or disclose the information.
d. A UH Covered Component may terminate a restriction if the individual agrees to it, or the UH Covered Component informs the individual of the termination.
e. A UH Covered Component must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if: (1) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (2) the PHI pertains solely to a health care item or service for which the individual or person other than the health plan on behalf of the individual, has paid the covered entity in full.

20. Access of individuals to PHI.
    a. In general, an individual has a right of access to inspect and obtain a copy of the individual's PHI in a designated record set for as long as the PHI is maintained in the record set.
    b. A UH Covered Component may also deny an individual access without providing the individual an opportunity for review, in certain circumstances.
    c. In general, a UH Covered Component has 30 calendar days to respond to a request if the PHI is on site and 60 calendar days otherwise. Delays will need to be justified in accordance with HIPAA.
    d. A UH Covered Component must document the designated record sets that are subject to access by individuals, as well as designate a person or office responsible for receiving and processing requests.
21. Amendment of PHI. An individual has the right to have a UH Covered Component amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set with exceptions as provided under HIPAA.
22. Accounting of disclosures of PHI. An individual has a right to receive an accounting of disclosures of PHI made by a UH Covered Component in the six years prior to the date on which the accounting is requested, with a few exceptions as provided in HIPAA.
23. Administrative requirements. Any and all local operating policies and procedures established by the UH Covered Component must be consistent with this System-wide HIPAA Policy and HIPAA.
    a. A UH Covered Component must designate a privacy official (e.g., Unit HIPAA Coordinator) who is responsible for the development and implementation of the local operating policies and procedures of the UH Covered Component that are consistent with this System-wide

HIPAA Policy and HIPAA, as well as a contact person/office who is responsible for receiving complaints.

b. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must train all members of its workforce on the policies and procedures with respect to PHI, as necessary and appropriate for the members of the workforce to carry out their functions within the UH Covered Component. Training must be documented.
c. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. (*See* safeguards specified in paragraph III.D herein.)
d. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must provide a process for individuals to make complaints and complaints must be documented.
e. Subject to consultation with and review and approval by the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures, and must document such sanctions. Sanctions are to be conducted in accordance with appropriate University policies and procedures and applicable collective bargaining agreements.
f. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must mitigate any harmful effects caused by the inappropriate disclosure of PHI.
g. A UH Covered Component must refrain from intimidation or retaliation against an individual for the exercise of an established individual right.
h. A UH Covered Component may not require individuals to waive their rights under the HIPAA regulations as a condition of the provision of treatment, payment, and enrollment in a health plan, or eligibility for benefits.
i. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements, and that are consistent with this System-wide HIPAA Policy and HIPAA. Revisions must also be made to policies and procedures as necessary to comply with changes in law.
j. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must maintain policies and procedures in written or electronic form; if a communication is required to be in writing, maintain such writing, or an electronic copy, as documentation; and if an action, activity, or designation is required to

be documented, maintain a written or electronic record of such action, activity, or designation.

D. **Security Policies and Procedures**

In addition to complying with the HIPAA Security Rule, the UH Covered Component must also comply with the University's Executive Policy EP 2.214, as amended. If the security provisions of this HIPAA Policy conflict with another University policy or procedure, the higher level of security protection must be followed by the UH Covered Component.

1. UH Covered Component mandatory security requirements. UH Covered Component must:
   a. Ensure the confidentiality, integrity, and availability of all its PHI;
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of the PHI, including ePHI;
   c. Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required;
   d. Ensure HIPAA compliance by its workforce.

2. HIPAA Security Rule specifications. Specifications in the HIPAA Security Rule are either "Required" or "Addressable". Required specifications must be implemented and addressable specifications must be assessed and implemented as specified if deemed reasonable and appropriate to the UH Covered Component.

3. Administrative safeguards. The following are required of all UH Covered Components and apply to employees, students and volunteers in the UH Covered Component. Any and all local operating policies and procedures established by the UH Covered Component must be consistent with this System-wide HIPAA Policy and HIPAA.
   a. With the assistance of the UH System HIPAA Privacy and Security Officer(s), implement policies and procedures to prevent, detect, contain and correct security violations. This includes: risk analysis, risk management, sanction policy, and information system activity review (*see* 45 CFR § 164.308(a)(1)(ii)(A)-(D)). Sanctions are to be conducted in accordance with appropriate University policies and procedures and applicable collective bargaining agreements.
   b. Identify the security official (e.g., Unit HIPAA Coordinator) who is responsible for the development and implementation of the policies and procedures required by this HIPAA Policy and the HIPAA Security Rule.
   c. With the assistance of the UH System HIPAA Privacy and Security Officer(s), implement policies and procedures to ensure that only

appropriate members of its workforce including students and volunteers have access to the PHI.

d. With the assistance of the UH System HIPAA Privacy and Security Officer(s), implement policies and procedures for authorized access to PHI.
e. With the assistance of the UH System HIPAA Privacy and Security Officer(s), implement a security awareness training program for all members of its workforce (including management, students and volunteers).
f. With the assistance of the UH System HIPAA Privacy and Security Officer(s), implement policies and procedures to address security incidents.
g. With the assistance of the UH System HIPAA Privacy and Security Officer(s), establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence, e.g., fire, vandalism, system failure, and natural disaster, that damages systems that contain PHI.
h. Perform periodic technical and non-technical evaluations to ensure that standards continue to be met in response to operational and environmental changes affecting the security of PHI.

4. Physical safeguards. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must:

   a. Implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.
   b. Implement policies and procedures that specify the proper functions to be performed, manner in which functions are to be performed, and physical attributes of the surroundings of a specific workstation/workstations that can access PHI.
   c. Implement physical safeguards for all workstations that access PHI to restrict access to authorized users.
   d. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into, out of and within the facility.

5. Technical safeguards. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must:

   a. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

b. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
c. Implement policies and procedures to protect PHI from improper alteration or destruction.
d. Implement procedures to verify that a person or entity seeking access to PHI is the one claimed.
e. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

6. Policies and procedures and documentation requirements. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component must:

   a. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements. This standard is not to be construed to permit or excuse action that violates them.
   b. Maintain policies and procedures implemented in written (may be electronic) form, and if an action, activity, or assessment is required to be documented, maintain a written (may be electronic) record of it.
   c. Retain the documentation required by paragraph (b) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

7. Notification in the Case of Breach of Unsecured PHI.

   a. Notification to individuals. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component shall, following the discovery of a Breach (as defined by HIPAA) of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the UH Covered Component to have been, accessed, acquired, used, or disclosed as a result of such Breach without unreasonable delay and in no case later than 60 calendar days following the discovery of such Breach. A Breach shall be treated as discovered by a UH Covered Component as of the first day on which such Breach is known to the UH Covered Component, or, by exercising reasonable diligence would have been known to the UH Covered Component. A UH Covered Component shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of the UH Covered Component (determined in accordance with the federal common law of agency).

b. Notification to others. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component shall also notify prominent local media outlets if the Breach involves more than 500 residents of the State no later than 60 calendar days after discovery of the Breach. (Shorter time frames may apply as required by law.)
c. Notification to the DHHS Secretary. With the assistance of the UH System HIPAA Privacy and Security Officer(s), a UH Covered Component shall notify the DHHS Secretary of Breaches on an annual basis, in a manner specified on the DHHS Web site, and via a report due to the DHHS Secretary no later than 60 calendar days after the end of the calendar year in which the Breaches are discovered *if less than 500 individuals are involved*. *If 500 or more individuals are involved*, the UH Covered Component shall notify the DHHS Secretary in the manner specified on the DHHS Web site, which presently requires notice without unreasonable delay and in no case later than 60 days following a Breach. (Shorter time frames may apply as required by law.)
d. Notification by a Business Associate. A Business Associate shall notify a UH Covered Component of a Breach within five (5) business days that the Business Associate discovered a Breach occurred or by exercising reasonable diligence would have been known to the UH Covered Component. A UH Covered Component shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of the Business Associate (determined in accordance with the federal common law of agency).
e. Notification to and coordination with UH System HIPAA Privacy and Security Officer(s). In the event of a Breach of PHI, the UH Covered Component must immediately notify the UH System HIPAA Privacy and Security Officer(s); cooperate with the System HIPAA Privacy and Security Officer(s), Chief Information Security Officer, and others in the course of the investigation of the Breach; and in coordination with the System HIPAA Privacy and Security Officer(s), initiate corrective action plans or other remediation or mitigation to prevent recurrence of the Breach or similar Breaches.

E. **University System HIPAA Privacy and Security Officer(s) and Unit HIPAA Coordinators**

1. Office of the Vice President for Information Technology and Chief Information Officer (OVPIT). The University has designated staff in OVPIT to serve as the University System HIPAA Privacy and Security Officer(s)

("UH System HIPAA Privacy and Security Officer(s)").

2. UH System HIPAA Privacy and Security Officer(s). The UH System HIPAA Privacy and Security Officer(s) is delegated responsibility for the development, implementation, and maintenance of this HIPAA Policy, in consultation with the University's Chief Information Officer and Chief Information Security Officer, and including all University privacy and security policies and procedures relating to HIPAA.
    a. Responsibilities relating to the HIPAA Privacy Rule. The UH System HIPAA Privacy and Security Officer(s) will be responsible for overseeing and managing the implementation of the HIPAA Privacy Rule. The UH System HIPAA Privacy and Security Officer(s) will assist the Unit HIPAA Coordinators in carrying out this HIPAA Policy and any University policies and procedures related to the HIPAA Privacy Rule, including but not limited to the following:
        1) Maintaining ongoing communication with all Unit HIPAA Coordinators;
        2) Coordinating training programs for the designated UH Covered Components (employees, students and volunteers) in cooperation with the Unit HIPAA Coordinators;
        3) Maintaining ongoing communications with the IRB regarding research use of PHI and Limited Data Sets;
        4) Responding to complaints regarding University policies, procedures and practices related to the privacy of health information; and
        5) Responding, or referring, to the appropriate UH Covered Component, requests by individuals for access and amendment, an accounting of disclosures, or requested restrictions to the use and disclosure of PHI.
        6) Approving and executing all BAAs, Data Use Agreements, and Data Sharing Agreements.
    b. Responsibilities relating to the HIPAA Security Rule. The UH System HIPAA Privacy and Security Officer(s) will be responsible for overseeing and managing the implementation of the HIPAA Security Rule, and will assist the Unit HIPAA Coordinators in carrying out this HIPAA Policy and any University policies and procedures related to the HIPAA Security Rule (including the security of PHI under HIPAA), including but not limited to the following:
        1) Maintaining ongoing communication with the Unit HIPAA Coordinators;
        2) Guiding and assisting with the development and implementation of ongoing security awareness and training programs for the employees, students, and volunteers of each UH Covered Component;
        3) Monitoring the use of security measures to protect PHI; and

4) Assisting in revising this HIPAA Policy and any University policy or procedure related to the privacy and security of PHI, as required to comply with changes in any applicable law, as well as documenting any change to any policy or procedure related to the privacy and security of PHI.

3. Unit HIPAA Coordinators. Each designated UH Covered Component must designate a Unit HIPAA Coordinator to assist the UH System HIPAA Privacy and Security Officer in carrying out this HIPAA Policy and all University policies and procedures related to the privacy and security of PHI and ePHI under HIPAA.

   Responsibilities of the Unit HIPAA Coordinators include, but are not limited to:

   a. Performing the role of liaison and maintain ongoing communication with the UH System HIPAA Privacy and Security Officer(s);
   b. Developing and maintaining procedures consistent with this HIPAA Policy for protection of PHI and ePHI in the University Unit, which is considered a UH Covered Component;
   c. Maintaining and updating, as needed, procedures consistent with the policy for protection of PHI and ePHI in the University Unit;
   d. Informing employees, volunteers, students, and as needed, consultants and others, about this HIPAA Policy and all University policies and procedures relating to HIPAA through various methods including but not limited to staff meetings, in person meetings, seminars, orientation meetings and phone or web based meetings;
   e. Monitoring the process of identifying and training new employees, volunteers and students within the University Unit who require access to PHI;
   f. Monitoring compliance with the policies and procedures of the University Unit relating to HIPAA;
   g. Reporting directly to the UH System HIPAA Privacy and Security Officer(s), any and all violations that result in an impermissible use or disclosure of PHI and/or ePHI;
   h. Reporting directly to the UH System HIPAA Privacy and Security Officer(s), any and all privacy violations under HIPAA;
   i. Reporting directly to the UH System HIPAA Privacy and Security Officer(s), any and all security violations under HIPAA;
   j. Ensuring continued compliance with HIPAA, this HIPAA Policy, and all University policies and procedures relating to HIPAA; and
   k. Reviewing all BAAs, Data Use and Data Sharing Agreements prior to execution by the Project Principal Investigator or Program Lead.

4. The responsible Unit HIPAA Coordinators for the UH Covered Components are listed on the University HIPAA Policy website: http://www.hawaii.edu/infosec/hipaa

F. **Authority for Signing of Business Associate Agreements, Data Use Agreements, and Data Sharing Agreements**

All BAAs, Data Use Agreements, and/or Data Sharing Agreements must be reviewed by the relevant Unit HIPAA Coordinator and the UH System HIPAA Privacy and Security Officer(s) in consultation with the University Office of the General Counsel as needed prior to execution.

With respect to BAAs, such prior review and consultation are not required if the UH Covered Component uses a standard University BAA template "as is" with no changes. *See* Attachments 3-A and 3-B.

Every BAA, Data Use Agreement, and Data Sharing Agreement must include the following approvals/signatures:

1) Project Principal Investigator or Program Lead;
2) UH System HIPAA Privacy and Security Officer(s) (or as otherwise delegated by OVPIT); and
3) Campus Chancellor (or designee) for campus projects, or appropriate System Vice President (or designee) for System projects.

## IV. Delegation of Authority

There is no policy-specific delegation of authority.

## V. Contact Information

Office of the Vice President for Information Technology & Chief Information Officer
hipaa@hawaii.edu
(808) 956-3501

## VI. References

A. Link to superseded policies: None

B. List of sources which relate to or impact the policy:

1. The Health Insurance Portability and Accountability Act of 1996, as amended (Pub. L. 104–191, 110 Stat. 1936 (1996) and affected/amended statutes), and implementing regulations (45 CFR Parts 160, 162 and 164)
2. The American Recovery and Reinvestment Act of 2009, as amended (Pub. L. 111–5, 123 Stat. 116 (2009) and affected/amended statutes), specifically including the Health Information Technology for Economic and

Clinical Health Act, as amended (42 U.S.C. §§ 300jj *et seq.*; 42 U.S.C. §§ 17901 *et seq.*).

3. 42 CFR Part 2, *Confidentiality of Alcohol and Drug Abuse Patient Records.*
4. HRS §§ 327E-2; 577-1, -25; 577A-1 to -3, -26; 577D-1 to -2.

C. Link to Executive Policy EP 2.214, *Security Protection and Sensitive Information*, as amended

http://www.hawaii.edu/policy/index.php?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=214&menuView=closed

## VII. Exhibits and Appendices

A. Attachment 1-A – University Authorization Template
B. Attachment 1-B –University Consent Template
C. Attachment 2 – University Notice of Privacy Practices Template
D. Attachment 3-A – University BAA Template (Unit is the Covered Entity)
E. Attachment 3-B – University BAA Template (Unit is the Business Associate)

**Approved:**

Signed _____ July 10, 2017
David Lassner Date
President