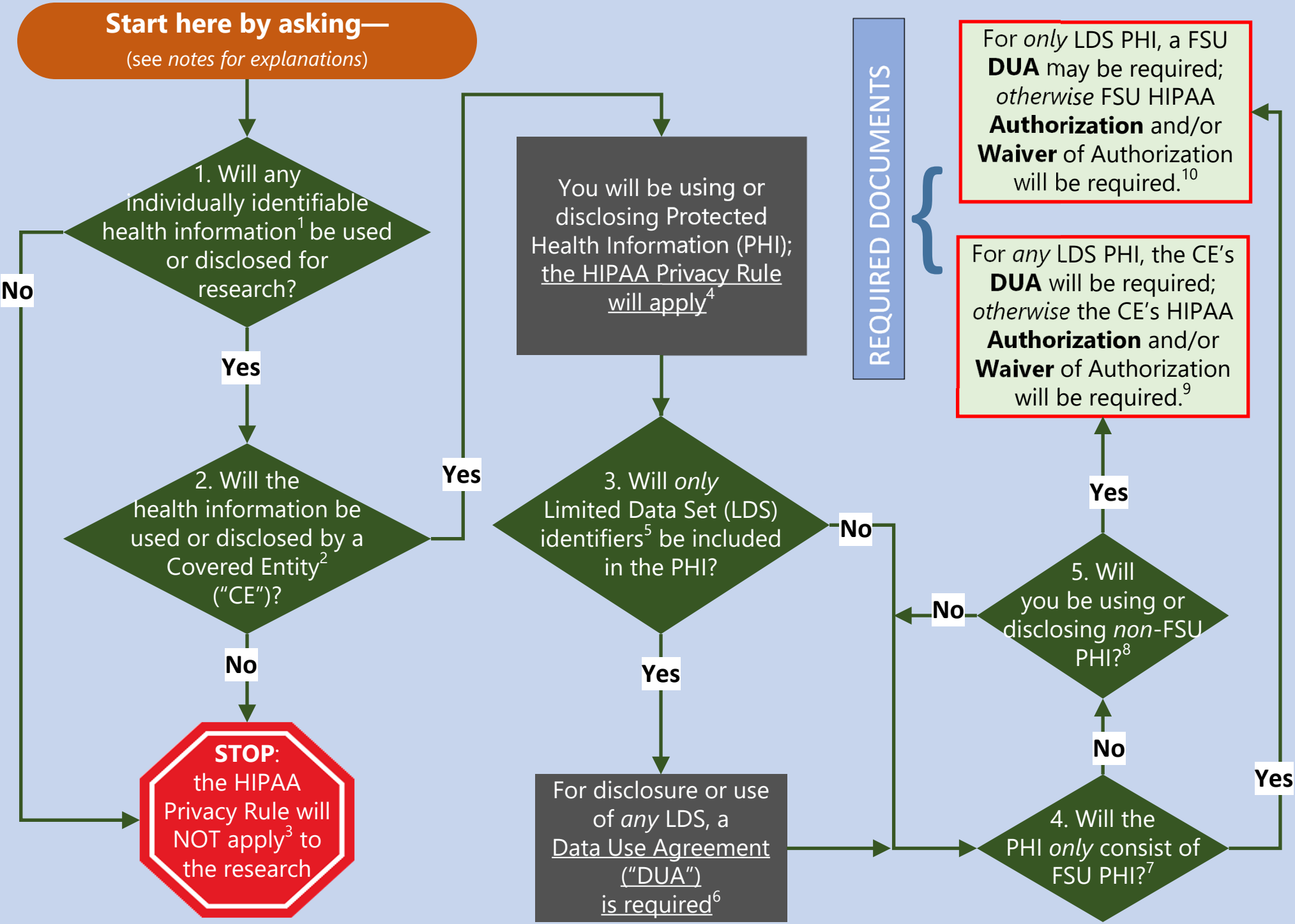
HIPAA Privacy Rule & Research: FSU Requirements (OHSP, March 17, 2022)



NOTES

1 *Individually identifiable health information* is defined under federal law as: 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; and,

(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,

(i) that **identifies*** the individual; or,

(ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual (Title 45 of the U.S. Code of Federal Regulations (CFR) Part 160 (45 CFR 160), section 160.103).

To locate a citation see https://www.ecfr.gov/ and search for the referenced Title and sections. The eCFR is not an official edition of the CFR but is more readily accessible and may be more current.

***Identifiers** of individuals OR of their relatives, employers, or household members include ANY of the following: (A) names; (B) geographic subdivisions smaller than a State; (C) all elements of dates (except year) for dates directly related to an individual, including birth, admission, discharge, treatment, death and all ages over 89; (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) service identifiers and serial numbers; (N) 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 (45 CFR 164.514(b)(2)(i)(A)-(R) and 164.514(b)(2)(ii)).

Answer "Yes" to this question 1 and proceed to question 2 if the health information that is used or disclosed includes ANY of the identifiers listed above OR (if there are no such identifiers) there is actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information; otherwise answer "No" and proceed as directed.

2 A *Covered Entity* means: (1) A health plan; (2) A health care clearinghouse; or (3) A health care provider who transmits any health information in electronic form in connection with a covered *transaction*. A covered *transaction* means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) Health care claims or equivalent encounter information; (2) Health care payment and remittance advice; (3) Coordination of benefits; (4) Health care claim status; (5) Enrollment and disenrollment in a health plan; (6) Eligibility for a health plan; (7) Health plan premium payments; (8) Referral certification and authorization; (9) First report of injury; (10) Health claims attachments; (11) Health care electronic funds transfers (EFT) and remittance advice; and (12) Other transactions that the Secretary may prescribe by regulation (45 CFR 160.103). Note that once a health plan, health care clearinghouse or health care provider is deemed a Covered Entity, then for purposes of

this algorithm it is irrelevant whether the health information that will be used by or shared with a researcher is transmitted in electronic or any other form, or ever used in connection with a covered transaction.

FSU may be considered a *hybrid entity*, which means a single legal entity, some activities of which include functions (referred to as covered functions) that are subject to the HIPAA Privacy Rule. If a FSU clinic or unit conducts certain covered functions, such as providing services, serving as a provider of medical or health services, and/or furnishing, billing or being paid for health care in the normal course of business, then the FSU clinic or unit is considered a health care provider, and as part of FSU the clinic or unit would be referred to as a health care component and subject to HIPAA Privacy Rule requirements. (45 CFR 164.103, 164.104(a)(3), 164.105(a)(2)(iii)(D)). Note that the term *health care provider* is expansive and may for example refer to outpatient services and supplies; psychologist services; clinical social worker services; medical nutrition therapy; diagnostic radiology tests; and durable medical equipment; also included are hospitals, skilled nursing facilities, comprehensive outpatient rehabilitation facilities, home health agencies, hospice programs or funds to pay for certain patient services provided in teaching hospitals or medical schools.

Answer "Yes" to this question 2 if the health information will be used or disclosed by a Covered Entity or health care component, and proceed to the explanation about Protected Health Information. Otherwise answer "No" and proceed as directed. However, if you are unsure about whether any particular FSU clinic or unit is a health care component do not answer "No" until you have first contacted the clinic or unit's legal counsel or privacy officer to obtain definitive information about the clinic or unit's HIPAA Privacy Rule status. The IRB may require this documentation as part of its review of research.

3 FSU would not be subject to federal HIPAA Privacy Rule enforcement action if health information that is used or disclosed for a research purpose is (1) NOT individually identifiable or (2) NOT used or disclosed by a Covered Entity (45 CFR 164.514(b)(2)(i)(A)-(R), 164.514(b)(2)(ii), 164.502(a)). Important note: if there is actual knowledge that the use or disclosure of de-identified information could be used alone or in combination with other information to identify an individual who is the subject of the information, then the HIPAA Privacy Rule will apply. Note also that compliance with other privacy and confidentiality laws or policies may still be required (e.g., Family Educational Rights and Privacy Act (FERPA) (pertaining to student education records); Privacy Act of 1974 (pertaining to federal agency systems of records); European Union General Data Protection Regulation (pertaining to the use and transfer of EU personal data)).

4 Individually identifiable health information that is used or disclosed by a Covered Entity or health care component is categorically Protected Health Information ("PHI"). Such use or disclosure of PHI for research purposes is subject to the HIPAA Privacy Rule (45 CFR 160.102(a)(1)-(3), 164.102(a)(1)-(3)). There are only a few exceptions, including e.g., PHI contained in Family Educational Rights and Privacy Act (FERPA)-protected education records; employment records held by a Covered Entity in its role as an employer; and regarding an individual who has been deceased for more than 50 years (45 CFR 160.103 ("Protected Health Information" definition)). Violations of any HIPAA Privacy Rule requirement are subject to civil monetary penalties, including between $10,000-$50,000 for each violation and up to $1.5 million for identical violations during any calendar year; each use of disclosure of PHI for a single individual which constitutes a violation of the HIPAA Privacy Rule is considered a single violation, and thus may be subject to a civil monetary penalty of between $10,000-$50,000 (45 CFR 160.400, 404). *Proceed to question 3*.

5 A Limited Data Set ("LDS") is PHI that excludes 16 of the 18 direct identifiers of the individual OR of relatives, employers and/or household members of the individual (see Note 1 above, "**Identifiers**"). A LDS may include ONLY 2 direct identifiers: (1) geographic information that only includes town or city, State and ZIP code, and/or (2) dates that are directly related to an individual (e.g., birth date, admission date, discharge date, service dates) (45 CFR 164.514(e)(2)). *If the PHI*

will include only these two identifiers, answer "Yes" to this question 3 and proceed to the explanation about Data Use Agreements. If the PHI will include other identifiers, answer "No" and proceed to question 4.

6 A Limited Data Set ("LDS") may be used or disclosed for purposes of research but ONLY IF a Data Use Agreement ("DUA") is first put into place (45 CFR 164.514(e)(4)). The DUA must include an assurance that the recipient of the LDS (e.g., researcher) will only use or disclose the protected health information for limited research purposes. Specifically, the DUA must contain the following elements:

(A) establish the permitted research uses and disclosures of the LDS by the researcher recipient and prohibit the researcher from using or further disclosing the information in a manner that would violate the HIPAA Privacy Rule;

(B) establish who is permitted to use or receive the LDS; and,

(C) provide that the LDS researcher recipient will: not use or further disclose the LDS other than as permitted by the DUA or as otherwise required by law; use appropriate safeguards to prevent use or disclosure of the LDS other than as provided for by the DUA; promptly (within 5 days of becoming aware of the incident) report to the Covered Entity and the IRB any incident involving use or disclosure of the LDS not provided for by DUA; ensure that any persons or entities to whom a researcher recipient provides the LDS as stipulated under the DUA agree to the same restrictions and conditions that apply to the LDS researcher recipient with respect to the LDS; and not identify the information or contact the individuals to whom the LDS pertains.

Even when use or disclosure of a LDS is accompanied by a DUA, FSU IRB review and approval of the study is still required; the IRB will require evidence of a suitable DUA as a condition of approval. Refer to the OHSP HIPAA Forms page [link] to obtain the FSU DUA template for use or disclosure of a LDS involving FSU PHI; for use or disclosure of a non-FSU Covered Entity's PHI, a DUA provided by the non-FSU Covered Entity may apply. *Proceed to question 4.*

7 Answer "Yes" to this question 4 and proceed as directed if the PHI that will be used or disclosed will consist of PHI that is *ONLY derived from FSU PHI* (i.e., the source of the PHI is only a FSU health care component, and NOT any non-FSU source of PHI, such as for example the Florida Department of Health, U.S. Centers for Medicare and Medicaid, Capital or other hospital, Tallahassee Orthopedic Clinic). Otherwise, answer "NO" and proceed to question 5. Note that this question 4 only pertains to PHI, not to other FSU or non-FSU information (health or otherwise) that may be used or disclosed for research purposes.

8 Answer "Yes" to this question 5 and proceed as directed if the PHI that will be used or disclosed will consist of BOTH FSU and a non-FSU Covered Entity's PHI, such as PHI that will be used or disclosed by the Florida Department of Health, U.S. Centers for Medicare and Medicaid, Capital or other hospital, Tallahassee Orthopedic Clinic). Otherwise, answer "NO" and then return to question 4 to confirm whether ALL the PHI that will be used or disclosed will consist of PHI that is only derived from FSU PHI. Note that this question 5 only pertains to PHI, not to other information (health or otherwise) that may be used or disclosed for research purposes.

9 Any PHI that is used or disclosed to a FSU researcher by a FSU Covered Entity or health care component *as well as by a non-FSU Covered Entity* will require that one or more of the following be provided for purposes of FSU IRB review:

(A) a executed (signed by all parties) Data Use Agreement (DUA) between the FSU researcher recipient and each Covered Entity or health care component (FSU and non-FSU) that is using or disclosing to the FSU researcher any Limited Data Set (LDS). Refer to the OHSP HIPAA Forms page [link] to obtain the FSU DUA template for use or disclosure of a LDS involving FSU PHI; non-FSU Covered Entities should have their own DUA templates to cover uses and disclosures of their PHI;

(B) a valid HIPAA Authorization form indicating that the individual about whom PHI pertains provides permission to use or disclose the individual's PHI for a research purpose (45 CFR 164.508). A HIPAA Authorization is required for use or disclosure for research purposes of any Covered Entity's PHI that is *not* a Limited Data Set (LDS) (i.e., the PHI consists of identifiers other than those permitted for a LDS) or for which use or disclosure a Waiver of HIPAA Authorization has not been approved (see (C) below). A HIPAA Authorization must contain specific required elements in order to be considered valid under the HIPAA Privacy Rule (45 CFR 164.508(b)(1), 164.508(c)). See the OHSP HIPAA forms page [link] to obtain the FSU template for a Research Authorization For Use and Disclosure of PHI;

While each Covered Entity may be expected to utilize its own HIPAA Authorization form that conforms to its circumstances (e.g., identifying the person(s) or class of persons at a Covered Entity who is authorized to make a disclosure of PHI), a single HIPAA Authorization form may be used for two or more Covered Entities, provided that all required elements are included in that HIPAA Authorization form. Also, a HIPAA Authorization may be combined with another authorization or consent form by which an individual provides permission to use or disclose their PHI for specifically research purposes (45 CFR 164.508(b)(3)); and/or,

(C) an approved waiver or alteration of HIPAA Authorization for the use and disclosure of PHI for research purposes, for which waiver or alteration an application or request is reviewed and approved by the Covered Entity' Privacy Board or IRB, and for which the Covered Entity's PHI is neither a LDS accompanied by a DUA nor expressly permitted under a valid HIPAA Authorization (45 CFR 164.512(i)(1)(i)). A Covered Entity Privacy Board or IRB's approval of an application or request for a waiver or alteration of HIPAA Authorization is an exception to the general requirement for a HIPAA Authorization, and may not be approved by a Covered Entity's Privacy Board or IRB unless specific requirements are satisfied. Also, while the FSU IRB may—upon a researcher's application—approve of a waiver or alteration of HIPAA Authorization, the FSU IRB does not approve of applications or requests for waivers or alterations for the use or disclosure of *non-FSU* PHI. This is because the non-FSU Covered Entity, *not FSU*, is legally responsible under the HIPAA Privacy Rule for use and disclosure of its own PHI. However, the FSU IRB will still require documentation of a non-FSU Covered Entity Privacy Board or IRB's approval of a waiver or alteration of HIPAA Authorization for use or disclosure for research purposes of the non-FSU Covered Entity's PHI. See the OHSP HIPAA forms page [link] to obtain the FSU template for an Application for Waiver or Alteration of Authorization for Use and Disclosure of PHI.

10 Any PHI that is used or disclosed to a FSU researcher by a FSU Covered Entity will require that one or more of the following be provided for purposes of FSU IRB review:

(A) an executed (signed by all parties) Data Use Agreement (DUA) between the FSU researcher recipient and the FSU health care component. Refer to the OHSP HIPAA Forms page [link] to obtain the FSU DUA template for use or disclosure of a LDS involving FSU PHI;

(B) a valid FSU HIPAA Authorization form indicating that the individual about whom PHI pertains provides permission to use or disclose the individual's PHI for a research purpose (45 CFR 164.508). A HIPAA Authorization is required for use or disclosure for research purposes of any FSU PHI that is *not* a Limited

Data Set (LDS) (i.e., the PHI consists of identifiers other than those permitted for a LDS) or for which use or disclosure a Waiver of HIPAA Authorization has not been approved (see (C) below). A HIPAA Authorization must contain specific required elements in order to be considered valid under the HIPAA Privacy Rule (45 CFR 164.508(b)(1), 164.508(c)). See the OHSP HIPAA forms page [link] to obtain the FSU template for a Research Authorization For Use and Disclosure of PHI (note that the FSU HIPAA Authorization form may be combined with another FSU authorization or consent form by which an individual provides permission to use or disclose their PHI for specifically research purposes (45 CFR 164.508(b)(3))); and/or,

(C) an approved waiver or alteration of HIPAA Authorization for the use and disclosure of FSU PHI for research purposes, for which waiver or alteration an application or request is reviewed and approved by the FSU IRB, and for which the FSU PHI is neither a LDS accompanied by a DUA, nor expressly permitted under a valid HIPAA Authorization (45 CFR 164.512(i)(1)(i)). The FSU IRB's approval of an application or request for a waiver or alteration of HIPAA Authorization is an exception to the general requirement for a HIPAA Authorization, and may not be approved by the FSU IRB unless specific criteria and other requirements are satisfied. See the OHSP HIPAA forms page [link] to obtain the FSU template for an Application for Waiver or Alteration of Authorization for Use and Disclosure of PHI.

(Revised March 17, 2022)