**ACCESSING CLINICAL DATA (PATIENT INFORMATION) FOR RESEARCH PURPOSES (HIPAA FAQs)**

BSPH researchers frequently need access to patient information for their research studies. Healthcare information in the United States is protected by federal and state laws and regulations, and by JHU institutional policies. This document is to help you understand what is necessary. It is important to know exactly what information you need, to seek only the “minimum necessary” to accomplish your research objective, and to follow the requirements outlined in this FAQ.

Note: Since BSPH is not a health care-providing institution and maintains no medical or billing records, unless a BSPH researcher has a joint appointment with the School of Medicine with clinical responsibilities, no BSPH researcher may access a medical record system – including Johns Hopkins Health System’s Epic – without specific approval from the BSPH IRB or the Johns Hopkins Medicine Privacy Office.

**What is HIPAA?**

The U.S. Health Insurance Portability and Accountability Act (HIPAA) provides national standards for protecting the privacy and security of health information and gives rights to individuals with respect to their health information. HIPAA regulates how health care organizations may use and disclose certain individually identifiable patient information, called protected health information (PHI).

**What is “Protected Health Information”, or “PHI”?**

If you use identifiable private information (e.g., clinical data or patient information) in your research, you have an obligation to protect the confidentiality of that information regardless of its source. HIPAA regulations are invoked when you wish to use individually identifiable health information that is created or received by a U.S. based “covered entity”. There are 18 identifiers that are included in the definition of PHI (see: <https://privacyruleandresearch.nih.gov/pr_08.asp>).

**What is a “covered entity”?**

Covered entities include organizations like health plans and healthcare providers who create, store, or transmit PHI electronically for treatment, payment, or operations purposes. For example, hospitals, academic medical centers, and other health care providers that electronically transmit claims to a health insurance company are covered entities – as is the insurance company. A covered entity may be an organization, an institution, or an individual. Pharmacies, health department clinics, physical therapists, acupuncturists, psychologists, and other private practitioners who bill for medication or treatment are all examples of “covered entities”. Johns Hopkins Hospital is a covered entity; **all** Johns Hopkins organizations providing health care to the public at their multiple delivery sites are “covered entities.”

**What is a “workforce member”?**

Employees, volunteers, trainees, and other persons whose work activities for the covered entity are under the direct control of the covered entity. The covered entity may require these individuals to sign a “workforce agreement” through which they promise to complete HIPAA training, comply with covered entity Confidentiality requirements and institutional policies, and not to use or disclose any PHI beyond what is needed to complete the work for the covered entity.

**Is the Johns Hopkins Bloomberg School of Public Health (BSPH) a covered entity?**

No, BSPH is not a covered entity. To have access to data from a covered entity, including the Johns Hopkins Hospital, you must seek permission from a HIPAA Privacy Board (see definition below). If you receive PHI disclosed by a covered entity you become just as responsible for protecting those data as is the covered entity. The approval process involves the submission of a research application to the BSPH IRB, which is authorized to review HIPAA applications as a HIPAA Privacy Board.

**What is a “disclosure” under HIPAA?**

Health care providers and other covered entities have the right to use patient information to treat patients, bill patients, and for any uses associated with conducting their operations. In general, a health care provider cannot “disclose” that information to anyone for any other purpose without either authorization from the patient or approval of a HIPAA Privacy Board. There are some exceptions for disclosures to law enforcement and public health authorities. Permitted disclosures must meet the “minimum necessary” standard; you only will get the PHI needed to accomplish your research purpose. Examples of disclosures include: looking into medical records to find people who might meet your study eligibility criteria; using text from medical records to develop algorithms to help identify patients with specific needs; and accessing and extracting information from medical records for cancer patients to link with state death registries. Just seeing someone’s name in a medical record is a “disclosure” by the covered entity.

A HIPAA breach is an improper disclosure, e.g. an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. HIPAA breaches have serious consequences. Intentional breaches, such as selling PHI for nefarious reasons, invite both criminal prosecution and civil penalties; breaches due to negligence may incur expensive fines. All breaches MUST be reported to the BSPH IRB office immediately.

**What is a HIPAA Privacy Board?**

A HIPAA Privacy Board is empowered to review research requests for HIPAA protected patient information. It consists of members with qualifications similar to those for an Institutional Review Board (IRB). The IRB’s HIPAA Privacy Board function overlaps with its ethical review function. The IRB reviews research applications that involve PHI and may approve the disclosure of PHI for research purposes through various mechanisms, including the following:

* a signed HIPAA privacy authorization,
* access to patient information in medical records to identify potentially eligible patients (also known under HIPAA as disclosures “Preparatory to Research”,
* the creation and use of a Limited Data Set,
* a HIPAA Waiver, and
* Representations for Research involving only Decedents’ Information.

**How can you access Johns Hopkins Medicine PHI for research purposes?**

Only clinicians who have a treatment relationship with a patient have the right to access PHI of their own patients. Other clinicians and faculty members must obtain IRB/Privacy Board approval for disclosures of PHI for research. There are five types of mechanisms through which disclosure for research may occur:

**Scenario 1:** **Preparatory to Research**. You are collaborating with clinicians in the School of Medicine (SOM) on a study about diabetes prevention and you want to identify adult patients aged 45-60 at Johns Hopkins Hospital and Bayview Medical Center who are pre-diabetic. Only JHH “Workforce Members” may access the electronic medical record system (Epic) to extract the names and contact information for potential research participants. The researcher must identify which Workforce Member(s) will access Epic. The permissible options are:

1. the JHH clinician co-investigator;

2. the Clinical Research Data Acquisition (CCDA) office (<https://ictr.johnshopkins.edu/programs_resources/programs-resources/i2c/center-for-clinical-data-analysis-ccda/>);

3. You, the BSPH researcher or a member of your research team, who is working at the direction of the JHH clinician and has an approved Workforce Agreement issued by the BSPH IRB/Privacy Board. Once you have the list of patients who may be potential study participants, you may work with the clinician-collaborator to send a communication to the potential participant that informs them about the study. HIPAA and institutional policy require that this communication must be from the clinician, not you. Note: The Workforce Agreement may not be used for any other Epic access. Access to Epic beyond this limited purpose is a HIPAA violation.

**Scenario 2:** **HIPAA Authorization**. You are planning a new study and are collaborating with clinicians at Johns Hopkins Medicine (JHM). You have secured permission to use a space outside the clinical/exam room to talk with patients who may be interested in becoming a participant. The study will involve an interview and access to medical record information. You must complete a BSPH HIPAA Application as part of your IRB application that identifies the specific data from the medical record that you want to access. You must also submit a Consent/Authorization Form to use to obtain from the participant both a signed informed consent for the study and a HIPAA Authorization allowing you to access their medical records.

It’s important to note that while a signed HIPAA Authorization from the participant gives permission for JHM to disclose PHI to you, it **does not** give you approval to access Epic. Only an authorized person or office inside the covered entity may access the PHI.

**Scenario 3: HIPAA Waiver**. You want to access pre-existing PHI (including names and social security numbers) for a secondary data analysis project from the JHM medical records to cross link with a Medicare dataset. The names and social security numbers are essential to linking the two data sets and will be replaced with a random identifier once the linkage is complete. You submit a BSPH HIPAA Application with your research submission to the IRB, requesting that the IRB waive the requirement for a signed HIPAA Privacy Authorization. If approved, you do not need to get a signature from each individual listed in that dataset to use their information. The BSPH IRB/Privacy Board will consider whether it is impracticable to do the research without the waiver, and whether the identifiers are essential to the research. If yes to both of these criteria, the IRB will approve the waiver as long as you take these additional steps:

1. An authorized person or office inside the covered entity must abstract the data from Epic: the JHM Core for Clinical Research Data Acquisition (CCDA) or a JH Privacy Office Approved Honest Broker (currently there is only one JHSPH employee who has this authorization).
2. If the number of records is over 500, you must obtain approval from the JHM Data Trust Research Sub-Council **prior to** final JHSPH approval. You will need to complete a JHM Data Security Profile and a Data Security Checklist with your application.
3. Your data security plan submitted with the research plan for the study is approved by BSPH Information Technology (IT).
4. If the number of records (i.e., participants) is below 50, you must enter information about the study in the JHSPH HIPAA compliance tracking database (<https://cfapps.jhsph.edu/SPH-JH-HIPAA-Compliance/>).

**Scenario 4: Limited Data Set**. You are doing a different type of secondary data analysis that only needs a limited about of PHI about eligible individuals: age, dates of service and zip code. These limited identifiers are permitted under HIPAA to be used for research without a HIPAA Privacy Authorization or HIPAA Waiver and qualify as a “limited data set”. You want this PHI from the Johns Hopkins Clinical Practitioners (JHCP) subgroup of JHM medical record data. You will need to meet the requirements listed in Scenario 3 above, with the exception of the last one, item d. There is no need to track disclosures with a limited data set. You must obtain approval from the JHCP review committee (separately, and in addition to, the BSPH IRB approval).

**Scenario 5:** **Representations for Decedents’ Only Research**. Although deceased individuals are not “human subjects” and use of their data does not require IRB oversight, HIPAA protects PHI of deceased individuals for 50 years after the date of death. If you wish to access a dataset comprised of data from only deceased individuals you must describe how the data will be used and protected. You will need to follow the same requirements of access and data security outlined in Scenario 1. The BSPH IRB website provides a link to the JHM HIPAA Form 5 that you must submit with your submission to the BSPH IRB.

**How do I access PHI for research from a non-Hopkins covered entity?**

BSPH faculty members must follow the HIPAA policies and requirements of non-Hopkins covered entities that may provide access to PHI for research; those policies and requirements may differ from what Hopkins requires. The BSPH IRB may serve as a HIPAA Privacy Board and make determinations for research using PHI from other institutions. Check with the data providing institution to find out how they would like to proceed; most data providers will require the JHU data researcher to enter into a Data Use Agreement. Consult with JHURA to execute that agreement.

**If I would like to use PHI from a covered entity in my research, what do I need to do?**

1. Complete one of the two BSPH IRB HIPAA applications:

* the BSPH IRB Application for Disclosure of Johns Hopkins Medicine (JHM) PHI, or
* the BSPH IRB Application for Disclosure of non-JHM PHI.

1. Submit the HIPAA application with your new PHIRST application or Amendment (if you are adding the access/use of PHI to an existing IRB approved study.) Include Authorization Forms, Workforce Agreements and Data Use Agreements, Data Security Checklist and Profile forms, and JHM HIPAA Form 5 as needed.

1. Ensure that your study team has completed the appropriate HIPAA training.

Still confused? Send us an email to [bsph.irboffice@jhu.edu](mailto:bsph.irboffice@jhu.edu).