Grand Valley State University
Institutional Review Board (IRB)
G-2: HIPAA Compliance, Coded Private Information, and De-Identified Data
Issued: December 8, 2021   Office of Research Compliance and Integrity

At GVSU, most research involving health information is conducted in collaboration with an external healthcare organization. In this guidance, "researcher" refers to any member of the IRB-approved research team.

1. <u>What is HIPAA? PHI?</u>
    HIPAA is the "Health Insurance Portability and Accountability Act." This federal law explains when protected health information may be used or disclosed by covered entities for research purposes. ***Protected health information*** (PHI) is any identifiable health information related to the care or treatment of a patient at a covered entity. ***Covered entities*** include medical clinics, hospitals, health insurance companies, and other institutions that create or process PHI. Any time PHI will be used or accessed for research purposes, permission from the patient is required, unless the IRB has granted a waiver of HIPAA authorization (see #4 below).

2. <u>When does HIPAA apply to research?</u>
    When a researcher wants to use PHI from a covered entity, HIPAA protects the information. If researchers have access to PHI due to their roles providing healthcare for patients, specific authorization is required to access the PHI for research purposes. Healthcare professionals do not have permission to access this information for research simply because of their roles on the healthcare team.

3. <u>Obtaining HIPAA authorization</u>
    The required elements of HIPAA authorization can be incorporated into the research informed consent form, or the HIPAA authorization can be a separate document. Before initiating a study, the researcher should contact the covered entity to determine if they will accept a combined consent and authorization, or if patients are required to sign the covered entity's HIPAA authorization forms (also referred to as a HIPAA Release of Information). The GVSU IRB has a HIPAA authorization template available here. If the HIPAA authorization will not be incorporated into the consent form, it still requires IRB review because it is part of the research informed consent process.

    The required elements of HIPAA authorizations are found in Appendix A.

4. <u>Waivers and alterations of HIPAA authorization</u>
    In certain circumstances, it may be appropriate for the researchers to request a waiver or alteration of the HIPAA authorization.

HIPAA waivers are most commonly sought for research involving a retrospective medical chart review with no patient interaction because it is often extremely difficult or impossible for the researchers to contact the individuals whose medical information is being accessed in order to complete the authorization. In the IRB initial protocol application, the researcher will need to explain why the waiver is necessary to conduct the research. The IRB may approve or deny the waiver request. If the request is denied, the researcher is required to obtain HIPAA authorization from the research subjects.

In other cases, an alteration to HIPAA authorization may be necessary for the research to occur. For example, if the research involves the review of medical records along with remote interviews of research subjects, the researcher may request to waive the requirement to obtain a signed authorization. The researcher must first obtain permission from the covered entity to obtain verbal HIPAA authorization before the IRB will consider this request. If documentation is waived, researchers are still expected to provide the research subject with a HIPAA information sheet containing all other required elements of HIPAA authorization.

The criteria that need to be satisfied to be granted a waiver or alteration of HIPAA authorization are found in Appendix B.

5. <u>Types of data sets, honest brokers, and data use agreements</u>
   De-identified data is data that has been stripped of all identifying information and for which there is no means by which it could be linked back to the subjects from whom it was originally obtained.

   The most common way to de-identify a data set is to permanently remove all 18 identifiers listed in the HIPAA regulations; this list of identifiers is found in Appendix C. Data that has all 18 identifiers removed is no longer considered PHI and no longer subject to HIPAA. This is now considered a de-identified data set because there is no way to later re-identify the data.

   Another method to achieve de-identification is the "Expert Determination" method. This expert is a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. The expert then applies these principles and methods to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by the recipient to identify an individual included in the data set. The expert then documents the methods used and the results of the analysis to justify this determination. Please consult the [Health and Human Services website](#) for further information regarding this method.

   Covered entities commonly utilize ***honest brokers*** to provide de-identified data to researchers. An honest broker is a neutral third party, who is not a member of the research team, and who has routine access to the PHI for operational purposes. In many cases, an honest broker attestation (see Appendix D for an example) is utilized.

Some covered entities will create a **coded data set** for researchers using an honest broker. These data sets are devoid of all identifiable information, and the honest broker creating the data set retains a correlation between an assigned random ID number and the patients' medical records. This allows the honest broker to re-identify the data set in case the researcher needs to come back and request some additional data points that weren't included in the original data set. Coded data sets are not considered PHI, but are still considered identifiable because the ability to later re-identify the data still exists.

A **limited data set** is a data set in which most of the PHI has been removed, except it can include dates (e.g. admission date, discharge date, date of service, date of birth), and city, state and ZIP code. Limited data sets are still considered PHI and are not considered de-identified data.

The covered entity providing the limited data set may require the researcher to complete a **data use agreement** (DUA). A DUA may not be needed if the researcher is part of the covered entity, either as an employee or as a student completing an internship or clinical rotation. If a DUA is needed, it cannot be signed by the researcher. These must be signed by the GVSU Vice Provost of Research Administration because the DUA is between GVSU and the covered entity; it is not an agreement between the researcher and the covered entity. A copy of GVSU's current DUA template agreement can be obtained from the Technology Commercialization Office.

6. HIPAA/IRB Requirements by Type of Data Set Provided by Covered Entity
The need for a HIPAA waiver or HIPAA authorization, as well as IRB review and approval, will depend upon the type of data set being used and the agreement(s) in place between the researchers and the honest broker. Please see the following table for details. Note that if a GVSU researcher will be the person creating the de-identified data set, the data set is considered identified because the researcher will be accessing identifiable information in order to create the de-identified data set.

	Identified Data Set	De-identified Data Set	Coded Data Set	Limited Data Set
Contains PHI?	Yes	No	No	Yes
Considered Identifiable?	Yes	No	Not identifiable to the researcher; it is identifiable to the Honest Broker.	Yes
IRB Review Required?	Yes	No	No, if **all** of the following are true: 1. GVSU researchers cannot readily ascertain the identity	No, if GVSU researchers cannot readily ascertain

			of the individuals to whom the coded private data pertains 2. Researchers and the holder of the key have entered into an agreement prohibiting the release of the key to the researchers under any circumstances 3. The data was not collected specifically for the current research project through an interaction or intervention with living individuals, and the holder of the key is not a member of the research team. Otherwise, yes.	the identity of the individuals to whom the limited private data pertains Otherwise, yes.
HIPAA Authorization or Waiver Required?	Yes	No	No	No
DUA required by covered entity?	Sometimes	Not usually	Not usually	Usually
Honest Broker Attestation Recommended?	N/A	Yes	Yes	Yes

7. Data management
    Data sets containing PHI, including limited data sets, must be protected at all times. Refer to IRB Policy 730: Collection, Management and Security of Research Information and IRB Guidance Document G-16: Guidance on Data Management Requirements for Research Data, for detailed information. Under no circumstances can these data sets be re-released to any other person.

8. Medical case reports
    A medical case report is a detailed report of the symptoms, signs, diagnosis, treatment and follow-up of an individual patient or up to three patients.   Because case reports are a description of a patient's course of treatment, they do not meet the federal definition of research and generally do not require review by the IRB.

    A case series (more than 3 cases) generally meets the definition of research and requires submission of the IRB initial protocol application. Case reports and case series that go beyond reporting the progression and treatment of cases by completing a systematic analysis

designed to answer a research question are considered to be research. These are required to be submitted to the IRB for review prior to engaging in any research activity.

Case report authors do not need to submit an IRB initial protocol application. If an author wishes to have the project assessed by the IRB to verify it meets the definition of a case report, they should submit the IRB Research Determination Form in IRBManager. A formal letter will be issued documenting that the case report does not meet the federal definition of research and IRB oversight is not needed.

Many journals now require a letter, or other acknowledgement, from an IRB prior to publication of a case report. Specifically, they wish to know whether IRB approval was obtained or was not required for the described case. Investigators should inform the Office of Research Compliance and Integrity (ORCI) if a journal does not accept the formal determination letter.

Case reports for publication or presentation must not include any PHI unless the specific authorization of the patient has been obtained. Any use or disclosure of PHI must be done with authorization of the patient, or, if the patient is deceased, authorization of the patient's family. The covered entity responsible for the security of the medical record (hospital, clinic, physician practice group, etc.) should be consulted prior to submission of the case report to assure proper authorization was obtained.

9. Medical Device Studies
   Medical device studies fall under the purview of the Food and Drug Administration (FDA). The FDA requires IRB review for all in vitro diagnostic device studies involving human specimens or samples, even when the research does not include identifiers and the biospecimens cannot be linked to any identifying information. This requirement also applies to the use of leftover specimens that are not individually identifiable, including any remnants of human specimens collected for routine clinical care or analysis that would have otherwise been discarded. In vitro diagnostic devices are defined as reagents, instruments, and systems that are intended for use in the diagnosis of disease or other conditions, including a determination of the state of health, in order to cure, mitigate, treat, or prevent disease or its sequelae.

Appendix A: Core elements and required statements of HIPAA authorizations

Per the HIPAA Privacy Rule at 45 CFR 164.508(c), a valid authorization must be written in plain language and must contain the following:

Core elements:
- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure (i.e., who will access the information)
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure (i.e., who will receive the information)
- A description of each purpose of the requested use or disclosure
- An expiration date or expiration event that relates to the individual or the purpose of the use or disclosure
- Signature of the individual or their personal representative. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided

Required statements:
- The individual's right to revoke the authorization in writing
- The exceptions to the right to revoke and a description of how the individual may revoke the authorization
- The consequences to the individual of a refusal to sign the authorization
- The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by the HIPAA regulations

The research participant must be provided with a copy of the signed HIPAA authorization.

Appendix B: Criteria to waive or alter the HIPAA authorization

Per the HIPAA Privacy Rule at 45 CFR 164.512(i)(2)(ii), the researcher must sufficiently explain each of the following before a waiver or alteration of HIPAA authorization will be granted:

- The use or disclosure of PHI involves no more than minimal risk to the privacy of individuals.
- There is an adequate plan to protect the identifiers from improper use and disclosure.
- There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law.
- There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI for which an authorization or opportunity to agree or object is not required by the HIPAA Privacy Rule.
- The research could not practicably be conducted without the waiver or alteration.
- The research could not practicably be conducted without access to and use of the PHI.

Appendix C: HIPAA Identifiers

Per HIPAA Privacy Rule 45 CFR 164.514(b)(2), if the following identifiers of the patient and of their relatives, employers, or household members, are removed, the data set is considered to be de-identified:

1. Names;
2. 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:
   a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. 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;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Once the above 18 identifiers have been removed, the data set should be assessed to determine that none of the remaining information could be used alone or in combination with other information to identify an individual who is a subject of the information. Once this assessment has been completed, the data is sufficiently de-identified and is no longer protected by the HIPAA Privacy Rule.

Appendix D: Honest broker attestation

Independent Honest Broker Assurance Agreement

Study Title: _____

IRB # (if known): _____

Principal Investigator (PI): _____

To be completed by the individual who is de-identifying the data
(NOT a member of the research team)

Name of honest broker: _____

GVSU department, if applicable: _____

Email address: _____

Business phone number: _____

Additional comments or restrictions, if applicable: _____

By signing below, I agree/certify that:
1. I have routine access (as part of my job responsibilities) to the data and records being requested.
2. I have reviewed this project with the PI and agree to obtain, de-identify and, if applicable, to maintain a correlation code for data that will be subsequently accessed by the research team.
3. I will not provide, under any circumstances, the PI or any member of the research team with information that would permit the identification of research subjects.
4. I will not intervene or interact with identified research subjects during the conduct of this research.
5. I will maintain complete confidentiality of research subjects' private information.

_____   _____
Signature   Date

The original completed form will be kept by the honest broker. A copy is provided to the PI and is submitted with the IRB initial protocol application. For GVSU FERPA-protected data, this form will be made available to the Registrar's Office and the Office of Institutional Analysis upon request.