1. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law that governs Protected Health Information (PHI). It was enacted with the goal of allowing persons to qualify immediately for comparable health insurance coverage when they change their employment relationships and it became effective in 2003.

2. Why does Children’s National have a policy for Research HIPAA Privacy and Security?

Children’s National Health System is a covered entity under the Health Insurance Portability and Accountability Act (HIPAA). As employees of Children’s National, individuals conducting or assisting with research activities must comply with the HIPAA privacy and security rule and follow institutional policies and procedures to protect all health information that is individually identifiable.

3. What is the Role of the Institutional Review Board (IRB) with regards to HIPAA Compliance?

The Institutional Review Board (IRB) responsibilities include enforcement of protections of individual privacy and maintenance of confidentiality of identifiable information in the context of research at the time of initial review, amendments and continuing review of research projects. When a data breach occurs in the context of research, the IRB is responsible for the assessment of Unanticipated Problems related to data, privacy and confidentiality breaches.

4. What is Protected Health Information (PHI)?

Information that can be linked to a particular person (i.e., is person-identifiable) that arises in the course of providing a health care service and is incorporated in the medical record. Electronic and paper information is protected.
5. **What elements of information constitute PHI?**

The HIPAA Regulation Identifies 18 elements:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Name</td>
</tr>
<tr>
<td>2.</td>
<td>Any geographic subdivisions smaller than a State, including street address, city, county, precinct, ZIP code, their equivalent geocodes, except for the initial three digits of a ZIP code.</td>
</tr>
<tr>
<td>3.</td>
<td>All elements of dates (except year) directly related to an individual (e.g., date of birth, admission).</td>
</tr>
<tr>
<td>4.</td>
<td>Telephone numbers.</td>
</tr>
<tr>
<td>5.</td>
<td>Fax numbers.</td>
</tr>
<tr>
<td>6.</td>
<td>Electronic mail addresses.</td>
</tr>
<tr>
<td>7.</td>
<td>Social security numbers.</td>
</tr>
<tr>
<td>8.</td>
<td>Medical record numbers.</td>
</tr>
<tr>
<td>9.</td>
<td>Health plan beneficiary numbers.</td>
</tr>
<tr>
<td>10.</td>
<td>Account numbers.</td>
</tr>
<tr>
<td>12.</td>
<td>Vehicle identifiers and serial numbers, including license plate numbers.</td>
</tr>
<tr>
<td>15.</td>
<td>Internet Protocol (IP) address numbers.</td>
</tr>
<tr>
<td>16.</td>
<td>Biometric identifiers, including finger and voiceprints.</td>
</tr>
<tr>
<td>17.</td>
<td>Full-face photographic images and any comparable images.</td>
</tr>
<tr>
<td>18.</td>
<td>Any other unique identifying number, characteristic, or code.</td>
</tr>
</tbody>
</table>

6. **What is not PHI?**

Some research studies collect and use data that is person-identifiable because it includes personal identifiers such as name, address, video recordings. It is not considered to be PHI if:

- The data are not associated with or derived from a healthcare service event (treatment, payment, operations, medical records)
- The data are not entered into the medical records,
- The subject/patient will not be informed of the results.
- Research health information that is kept only in the researcher’s records is not subject to HIPAA but is regulated by other human subjects’ protection regulations.
- Health information by itself without the 18 identifiers is not considered to be PHI.
7. **How does HIPAA Impact Research?**

- HIPAA regulations allow researchers to access and use PHI when necessary to conduct research.
- HIPAA only affects research that uses, creates, or discloses PHI that was or will be entered into the medical record or will be used for healthcare services, such as treatment, payment or operations.
- HIPAA covers research on all human beings, **living or dead**, regardless of whether the research is supported by the federal government or regulated by the Food and Drug Administration (FDA).

8. **What is De-identified Health Information?**

De-identified health information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. Research involving only “de-identified data” is exempt from HIPAA regulations. De-identified information can be used and disclosed for research purposes without the authorization of the individual whose information is being used.

9. **How can health information be de-identified?**

PHI may be de-identified using either of two methods permitted by Federal law: 1) “safe harbor” method, and 2) statistical method. Children’s National accepts either method as a means of de-identifying PHI.

10. **What is the Safe Harbor method of PHI de-identification?**

- This method works by removing all 18 of the PHI identifiers of the subject, and of the subject’s relatives, employers and household members.
- The following exceptions are permitted:
  i. The initial three digits of the ZIP Code may be used.
  ii. The year element of dates directly related to a patient including birth date, admission date, discharge date, and date of death may be used.
  iii. Year of birth may not be used for subjects older than age 89. Their ages instead may be aggregated into a single category of age 90 or older.
11. Is removing identifiers always sufficient to de-identify PHI?

- No, information is not de-identified if the researcher has actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a participant.
- For example, it would not be acceptable to include year of birth if that information could readily be used to identify an individual due to the rarity of his/her condition. An example of how an individual might be identified even after removal of all identifying information is an unusual wound reported in a local newspaper.

12. How can I use the Statistical method of PHI De-Identification?

- Provide documentation that the research team will apply generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.
  a) Consult a qualified statistician or a person with appropriate knowledge and experience. The documentation should include:
    i. Determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify the patient who is a subject of the information, and
    ii. The methods and results that justify this determination

  OR

  b) Use an accepted HIPAA-compliant statistical program (for example: RedCAP).

13. How does the IRB determine if the research data set is de-identified?

- **Safe Harbor Method:** In addition to reviewing the description provided by the PI in the application, the IRB reviews the items in the case report or data collection form to ensure that no PHI is being collected.

- **Statistical Method:** The IRB reviews the statistical method and analysis included in the documentation. Investigators should use an accepted HIPAA-compliant statistical program or consult with the CRI Biostatistics and Informatics department.
14. I am collecting my research information in a de-identified manner but I am keeping a re-identification code. Is my research compliant with HIPAA regulations?

A re-identification code may be used to link identifiable PHI to a subject if it is not derived from information about the individual. The investigator must document how and when the re-identification code will be used and by whom, and the procedures for destruction of the code when it is no longer needed.

15. Is there a difference between Use and Disclosure of PHI?

- **Use** of PHI happens within a health care organization or covered entity. PHI is under direct control of that organization.
- **Disclosure** of PHI occurs when PHI is given to someone who is not part of the organization’s work force. (“Work force” includes employees, volunteers, contractors, and students of the health care organization).

16. What are the HIPAA-Compliant ways to use and disclose information?

- If an investigator and/or research staff must use identifiable PHI or disclose it to persons or organizations outside of Children’s National there are several ways this can be accomplished. They are:
  a) Written authorization from the patient or LAR
  b) Waiver of authorization
  c) Review preparatory to research
  d) Limited data set
  e) Decedent research

- IRB review and approval must be obtained prior to the use or disclosure of any identifiable information for the purposes of research.

17. Can a researcher review the totality of the chart of a patient during a research study?

- Requests for information for purposes that comply with the Privacy Rule will be assumed to be only the minimum necessary information. This is known as the “Minimum Necessary Standard.”
If the IRB does not agree that the amount of information requested is reasonably necessary for the purpose of the project, it is up to the IRB and the requesting investigator to negotiate to resolve their disagreement about the amount of information that is needed.

18. All patients at Children’s National have been informed that their medical information may be used for research and educational purposes. Why do I have to obtain a HIPAA Authorization?

- Research is separate from hospital operations. Therefore, a participant’s signature acknowledging receipt of the standard Children’s National “Notice of Privacy Practices” is not sufficient for research purposes.
- To comply with the HIPAA rule, a separate authorization must be obtained from every subject for any and all research activities involving PHI.

19. If I am obtaining informed consent, why do I need to obtain a HIPAA Authorization?

An informed consent document is an individual's agreement to participate in a research study and includes, among other things, a description of the study, anticipated risks and/or benefits, and how the confidentiality of records will be protected. In contrast, a HIPAA Authorization is an individual's signed permission to allow Children's National (a covered entity) to use or disclose the individual's protected health information (PHI) that is described in the authorization for research purposes.

20. What are the elements of a valid HIPAA Authorization?

There are 11 required elements for valid HIPAA Authorization. In general the main elements that should be included are:

- A description of the PHI that is discussed in the protocol.
- The name or identification of the persons or class of persons authorized to make and to receive disclosures of PHI for research-related purposes.
- A description of each purpose of the requested use or disclosure.
- An expiration date or event, or a statement such as “end of research study” or “none.”
- The individual’s signature (or that of his or her legally authorized representative) and date.

The HIPAA regulations state that a copy of the signed authorization must be given to the research subject (45 CFR 164.508 (c)(4)).
21. Can the HIPAA Authorization be combined with the consent form?

- Yes. HIPAA regulations permit an authorization for the use or disclosure of PHI for a research study to be combined with the written informed consent/parental permission document.
- The consent form templates approved by the Children’s National IRB include the elements and statements necessary for a valid HIPAA authorization.

22. How should I use the Children’s National HIPAA template?

- The investigator should modify certain template language in the HIPAA authorization to provide study-specific information.
- The investigator may not modify the HIPAA template language for use and disclosure of PHI without IRB review and approval.
- The IRB will not accept most sponsor or funding agency-initiated modifications to the Children’s National authorization language.

23. Can the requirement for HIPAA Authorization be Waived by the IRB?

A HIPAA waiver is generally required whenever a waiver of informed consent or a waiver of documentation of informed consent is requested.

The following criteria must be satisfied and documented in writing:

a) The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
   i. An adequate plan to protect the identifiers from improper use and disclosure.
   ii. An adequate plan to destroy the identifiers at the earliest opportunity.
   iii. Adequate written assurances that the PHI will not be reused or disclosed except as required by law.

b) The research could not practicably be conducted without the waiver or alteration; and

c) The research could not practicably be conducted without access to and use of the PHI.

24. Do I need HIPAA Authorization to use PHI to develop a research protocol?

- Yes. Before PHI is used, disclosed, or reviewed preparatory to research, the investigator must complete and submit the Authorization for Preparatory to Research form found in IRBear>Home>General Information>Forms and Templates to the Office for the Protection of Human Subjects (OPHS).
- This form should be submitted on its own if the investigator intends to use the PHI during the planning stages of the research. However, if the protocol is fully developed, the Preparatory to Research form should be included as part of the new protocol application.
25. Can I identify prospective research participants from medical records without their Authorization?

- The IRB may waive or alter the HIPAA authorization for the purpose of prescreening and identifying potential research subjects.
- An investigator must request such a waiver as part of a specific protocol application or, if the prescreening is to be used to identify potential subjects for multiple studies, as a stand-alone screening protocol.
- All requirements in the waiver application must be documented. Minimum Necessary Standard applies.

26. Can I contact prospective participants identified during a review preparatory to research?

- **NO.** If potential participants are identified during the preparatory process, they may not be contacted for enrollment until the protocol under development has been submitted as a new application, and reviewed and approved by the IRB.
- All recruitment methods should be reviewed and approved by the IRB prior to implementation.

27. What is a limited data set?

A limited data set must exclude all of the following direct identifiers of the individual or of the individual’s relatives, employers, or household members:

| a) Names | k) Vehicle identifiers and serial numbers, including license plate numbers |
| b) Postal address information other than town or city, State and ZIP code | l) Device identifiers and serial numbers |
| c) Telephone numbers | m) Web Universal Resource Locators (URLs) |
| d) Fax numbers | n) Internet Protocol (IP) address numbers |
| e) Electronic mail addresses | o) Biometric identifiers, including finger and voiceprints |
| f) Social security numbers | p) Full-face photographic images and any comparable images |
| g) Medical record numbers | q) Any other unique identifying number, characteristic, or code |
| h) Health plan beneficiary numbers | |
28. Can a researcher disclose a limited data set to an outside collaborator?

- An investigator who is authorized to have access to PHI may use or disclose a limited data set for research purposes without an authorization or waiver of authorization.
- A limited data set may be used or disclosed only if there is a Data Use Agreement between the covered entity and the recipient of the limited data set. A sample Data Use Agreement is available in IRBear. The Data Use Agreement will be prepared and approved by the Office of Grants and Contracts.

29. Can I disclose PHI to a research collaborator?

Yes, a valid Business Associate Agreement (BAA) must be in place before PHI may be disclosed to outside collaborators for purposes of:
- Preparing a limited data set for use by the covered entity or another recipient
- De-identifying data in the role of an “honest broker”
- Creating or maintaining a repository containing PHI
- Disclosing PHI to another covered entity

30. Can research be conducted with PHI from decedents under the HIPAA rule?

Before a decedent’s PHI is used or disclosed, the researcher must submit to the IRB a written request which includes:
- A statement that only PHI pertaining to decedents will be used or disclosed
- Documentation of the death of each individual whose PHI will be used or disclosed (if required by the IRB)
- Representation that the PHI sought is necessary for the research

31. Do research participants have access to PHI generated in the course of research?

- All research records pertaining to studies with Principal Investigators who are Children’s National Medical Center faculty and staff are the property of Children’s National.
- With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about them.
- One of the permitted exceptions applies to protected health information created or obtained by a covered health care provider/researcher for a clinical trial. The Privacy Rule permits the individual’s access rights in these cases to be suspended while the clinical trial is in progress, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial.
32. How do I properly protect PHI and research data generated in the course of research activities?

- Investigators are responsible for ensuring that effective procedures are in place to protect identifiable and confidential information collected for research purposes.
- Investigators and research staff should be familiar with the Children’s National Information Security Policies and work with the IT department if they have any questions or need guidance.

33. What are practical ways to protect PHI?

Investigators must collect only the minimum identity information needed and describe in the protocol exactly what personally identifiable data elements will be collected. The following steps should be taken:

- Remove/destroy identifiers as soon as they are no longer needed.
- If the data are electronic, the information must be encrypted during storage and decrypted only when needed for conduct of the research.
- Physically secure identifiers.
- Identifiers must be stored in a physically separate and secure location from the data files and the key to the code.
- Identifiers should not be stored on laptops, PDAs, flash drives or other portable devices. If it is necessary to use portable devices, these should be encrypted and the identifiers moved to a secure system as soon as possible.

34. Additional Steps to Protect Data

- Lock portable devices in a secure location when not in use.
- Identifiers transmitted over public networks must be encrypted.
- Identifiers and contact information cannot be distributed outside Children’s National without the specific consent of research participants and approval by the IRB.
- Limit physical and electronic access to identifiers to authorized research personnel.
- For additional information on computer security refer to the Children’s National IT security policies and guidance.

35. What should I do in case of a Data Breach?

Security breaches and unauthorized disclosures of research data or research subjects’ PHI should be reported to the IRB within one business day using the Reportable Event Module in IRBear.