CMS Data Use Agreements and Data Management Plans

HIPAA-P12

About This Policy

Effective Dates:
07-01-2014

Last Updated:
08-01-2016

Responsible University Administrator:
Vice President for University Clinical Affairs

Policy Contact:
University HIPAA Privacy Officer

Scope

This policy applies to all personnel, regardless of affiliation, who intend to use identifiable data from the Centers for Medicare and Medicaid Services (CMS) for research purposes under the auspices of Indiana University. CMS requires compliance with these rules regardless of whether the recipient is part of a covered entity. The recipient must comply with the final provisions of the security and privacy rules regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Policy Statement

Any researcher, research team or unit who will request identifiable data from CMS for research purposes must comply with this policy.

Data Use Agreement

Pursuant to the Board of Trustee Powers of Treasurer Resolution dated June 20, 1991, only the Treasurer of the Trustees of Indiana University and of the University and others acting in conjunction with the Treasurer are granted specific authority to execute certain documents on behalf of the University.
The Treasurer has designated the University HIPAA Privacy Officer to have signature authority for all Data Use Agreement (DUA).

The University HIPAA Privacy Officer will sign all CMS DUAs on behalf of the Trustees of Indiana University.

The University HIPAA Privacy Officer will review and approve all CMS DUAs.

The University HIPAA Privacy Officer will track all CMS DUAs. CMS DUAs will be tracked in REDCap database. Information recorded in REDCap will include:

1. DUA Number
2. Study Name/Title
3. IU’s IRB number, if applicable
4. Name of IU’s Principal Investigator
5. HIPAA training completed: Y/N
6. Confidentiality Agreement: Y/N
7. Date DUA signed
8. Date data received

9. Types of data received
10. Planned termination date
11. Date data are destroyed
12. Date Certificate submitted to CMS

The research team and collaborators will comply with all requirements setforth in the CMS DUA.

The research team and collaborators will not use the data received under the CMS DUA for any other purpose and will not use this data after the project is completed.

Data Management Plan

The Principal Investigator will be responsible for developing and maintaining the Data Management Plan as required by CMS.

Approval of Data Management Plan

IU's IRB will have responsibility to review all CMS Data Management Plans through the IRB protocol/study approval process:

- Initial review process;
- Continuing review process as designated in the IRB approval.

CMS will have final approval over all CMS Data Management Plans.

Confidentiality Agreement

The Principal Investigator will ensure all members of the research team review and sign a confidentiality agreement that binds each member and ensures the privacy and security of the data received.

Training

1. **CITI (Collaborative Institutional Training Initiative)**. All key personnel and any researcher directly interacting with human subjects are required to complete CITI training every three (3) years.
2. **HIPAA Privacy and Security & Notification Requirement Training**. Pursuant to Indiana University's HIPAA Privacy and Security Compliance Plan, each member of the research team will complete HIPAA training annually.
3. **Security of Mobile Devices Training**. Each member of the research team is required to complete Security of Mobile Devices training at least once. Employees will gain an understanding of how to properly protect information accessed or stored on mobile devices. The module also references Indiana University's IT 12.1 Mobile Device Security Standard.
4. **New Employee Compliance Orientation (NECO)**. All new employees in the Health Science Schools are required to complete NECO within 90 days of employment. New employees will gain an understanding of their obligations for compliance and will be provided with resources needed to address and report compliance matters.

Notification of project staffing changes:

1. Per Indiana University Standard Operating Procedures for Research Involving Human Subjects, Section 2.1.8, the Principal Investigator will ensure any changes in study team members will be reflected in the University IRB protocol.
2. The Principal Investigator will also notify CMS of any changes to the project staff listed on the CMS Executive Summary for Research Identifiable Data.

Notification of project staff or collaborator who terminate from the project:

1. Per Indiana University Standard Operating Procedures for Research Involving Human Subjects, Section 2.1.8, the Principal Investigator will ensure any terminations of study team members will be reflected in the University IRB protocol.
2. The Principal Investigator will notify CMS of any study team member or collaboration termination from the project.

3. The Principal Investigator will ensure access to CMS' data is terminated for any person who is terminates from the project.

Notification of project staff or collaborator who are terminated (voluntary or involuntary):

1. Per Indiana University Standard Operating Procedures for Research Involving Human Subjects, Section 2.1.8, the Principal Investigator will ensure any terminations of study team members will be reflected in the University IRB protocol.
2. The Principal Investigator will notify CMS of any terminations of study team members as well as collaborators.
3. The Principal Investigator will ensure access to CMS' data is terminated for any person who is terminated or terminates from the project.

Reporting Incidents and/or Breaches
Indiana University must notify CMS of any suspected incident wherein the security and the privacy of the CMS data may have been compromised.

1. Indiana University Policy ISPP-26, *Information and Information System Incident Reporting, Management, and Breach Notification*, outlines procedures for suspected or actual security breaches of information, attempts to compromise information, or weaknesses in the safeguards protecting information. Under this policy, all individuals encountering such information are required to immediately report to the University Information Privacy Office by phone or email to it-incident@iu.edu
2. The University HIPAA Privacy Officer has primary responsibility for reporting to federal agencies within seven (7) days if there is a suspected incident where the security and privacy of the CMS data may have been compromised, as outlined in Indiana University's incident response procedure.

Certificate of Disposition
CMS requires this certificate to be completed and submitted to CMS to certify the destruction/discontinued use of all CMS data covered by the listed DUA at all locations and/or under the control of all individuals with access to the data.

This includes any and all original files, copies made of the files, any derivatives or subsets of the files and any manipulated files. The requester may not retain any copies, derivatives or manipulated files. All files must be destroyed or properly approved in writing by CMS for continued use under an additional DUA(s). CMS will close the listed DUA upon receipt and review of this certificate and provide e-mail confirmation to the submitter of the certificate.

The Principal Investigator (PI) shall:

1. Complete & sign the CMS Certificate of Disposition;
2. Submit the signed Certificate to CMS;
3. Submit a copy to the University HIPAA Privacy Officer, by emailing a scanned copy to HIPAA@iu.edu

The University HIPAA Privacy Officer will record the date the Certificate was submitted to CMS in the REDCap database.

Reason For Policy

Indiana University is committed to protecting the privacy of health information as required under the HIPAA Privacy and Security Rules. HIPAA states PHI can only be used for specific research purposes pursuant to a HIPAA Authorization, a Privacy Board approved Waiver of Authorization or if an exception applies. A covered entity such as CMS, may enter into an agreement with another entity and share their PHI as long as they obtain assurances the data will be protected as required under law

Definitions

See HIPAA Glossary for a complete list of terms.

Sanctions

See HIPPA-G01 HIPAA Sanctions Guidance.

History

05/01/2016 Effective Date
02/15/2017 Updated Approval of Data Management Plan

Related Information

HIPAA-P02 Minimum Necessary Policy
HIPAA-P08: Removal and Transport of Protected Health Information
HIPAA Privacy and Security Compliance Documents