CMS Data Use Agreements and Data Management Plans

HIPAA-P12

About This Policy

Effective: 05/01/2016
Last Updated: 12/13/2021

Responsible University Office:
Office of the Chief Privacy Officer

Responsible University Administrator:
Chief Privacy Officer
mawerlin@iu.edu

Policy Contact:
HIPAA Privacy Officer
HIPAA Security Officer
hipaa@iu.edu

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. 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. CMS requires compliance with these rules regardless of whether the recipient is part of a covered entity.

Policy Statement

Any researcher, research team, or unit who will request Research Identifiable Files (RIFs) or Limited Data Sets (LDS) from CMS for research purposes must comply with this policy.

A. Data Use Agreement

1. The University Treasurer has designated the University HIPAA Privacy Officer to have signature authority for all CMS Data Use Agreements (DUAs).The University HIPAA Privacy Officer will review, approve, and sign all CMS DUAs on behalf of the Trustees of Indiana University.

2. The University HIPAA Privacy Officer will track and retain all CMS DUAs.

3. The research team and collaborators will comply with all requirements set forth in the CMS DUA.

4. 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.

B. Data Management Plan

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

2. Approval of Data Management Plan:
   a. IU's IRB will review all CMS Data Management Plans through the IRB protocol/study approval and continuous review process.

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

3. The Principal Investigator is responsible for ensuring all members of the research team review and understand their obligations for privacy and security of the data received.

C. 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 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.

D. Notification of Project Staffing Changes

1. The Principal Investigator will ensure any changes in study team members will be reflected in the University IRB protocol.

2. The Principal Investigator is responsible for notifying CMS of changes to the project staff listed on the CMS Executive Summary for Research Identifiable Data or when a study team member or collaborator terminates from the project.

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

E. Reporting Incidents and/or Breaches

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

2. 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.

3. 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.

4. 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/or privacy of the CMS data may have been compromised.

F. Certificate of Disposition

1. CMS requires a certificate of disposition 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.

2. This includes 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.

3. The Principal Investigator shall:
   a. Complete & sign the CMS Certificate of Disposition;
   b. Submit the signed Certificate to CMS;
   c. Submit a copy to the University HIPAA Privacy Officer;
   d. Email a scanned copy to: HIPAA@iu.edu.

4. The University HIPAA Privacy Officer will record the date the Certificate was submitted to CMS.

Reason for the Policy

Indiana University is committed to protecting the privacy of health information as required under the HIPAA Privacy and Security Rules. HIPAA states protected health information (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 Glossary of HIPAA Related Terms for complete list of terms.

History

05/01/2016 Effective Date
02/15/2017 Updated section II.A.
06/xx/2017 Published on University policy site
12/13/2021 Updated sections II.B and D, and removed IV.B.

Related Information

CMS Data Disclosures and Data Use Agreements (DUA)
US-CERT Federal Incident Notification Guidelines

HIPAA Privacy Rule
45 CFR 164.530(c)
45 CFR 164.530(e)

HIPAA Security Rule
45 CFR 164.310
45 CFR 164.310(d)(2)(i) and (ii)