



# INDIANA UNIVERSITY

## HIPAA–P11 Retention and Destruction of Protected Health Information

### FULL POLICY CONTENTS

Scope	<b>Effective:</b> July 1, 2015
Reason for Policy	<b>Last Updated:</b> August 1, 2016
Definitions	
Policy Statement	<b>Responsible University Office:</b>
Sanctions	<i>HIPAA Privacy and Security Compliance Office</i>
<b>ADDITIONAL DETAILS</b>	<b>Responsible University Administrator</b>
Additional Contacts	<i>Vice President for University Clinical Affairs</i>
Forms	
Related Information	<b>Policy Contact:</b>
History	<i>University HIPAA Privacy Officer</i>

### Scope

This policy applies to all personnel, regardless of affiliation, who create, access or store Personally Identifiable Information (“PII”) and Protected Health Information (“PHI”) at Indiana University, in accordance with the Privacy and Security Rules of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Please refer to the [IU HIPAA Affected Areas document](#) for a full list of departments impacted within Indiana University.

This policy covers PII and PHI in any form: electronic, paper, hardware, USB drives, CDs, etc.

### Reason for Policy

Protected health information in any form must be securely maintained, controlled and protected to prevent unauthorized access or disclosure. The purpose of this policy is to ensure that all records containing protected health information are retained and disposed of in accordance with the guidelines set forth by federal and state regulations.

---

## Definitions

See [Glossary of HIPAA Related Terms](#) for a complete list of terms.

---

## Policy Statements

It is the policy of Indiana University to retain records containing PHI in a usable, retrievable, and legal format for a period of time as mandated by IU policies and procedures, federal, state, and local governing authorities, whichever is more stringent.

### I. Record Retention:

Records may take the form of electronic medical record, paper documents, microfilm, electronic data storage, etc., and must be retained in such a way that the information is available for its intended business purposes. Records must be secured to prevent unauthorized access or disclosure and opportunities for loss and/or damage must be minimized.

- A. Medical records shall be retained for the full period of time required by state laws and/or IU policies.
  - Adult medical records will be retained for a minimum of seven (7) years from the last date of service.<sup>1</sup>
  - Pediatric medical records will be retained for a minimum of three (3) years beyond the age of majority.
- B. Records may be microfilmed or electronically scanned, with procedures in place to ensure the accurate and complete retrievable reproduction of the original document. (Scanned electronic images of the record become the original, official record immediately after creation and are retained in accordance with the applicable policy.)
- C. Research records that contain PHI may be governed by additional policies or regulations and shall be retained for the period of time required by the research protocol, research sponsor or funding agency or requirements of any associated research grant.

### II. Record Destruction and Disposal:

Destruction/disposal of records containing PHI will be carried out in accordance with IU policies and procedures, HIPAA regulations and federal and state laws.

- A. Each IU HIPAA Affected Area is responsible for arranging for the safe and secure destruction/disposal of records containing PHI and other critical or restricted information.
- B. Records shall not be destroyed/disposed of before the minimum retention period has been met.
- C. The destruction/disposal of any records must be approved by the IU HIPAA Affected Area responsible for the creation and/or retention of the records.

---

<sup>1</sup> IU Health policy states that “adult and pediatric patient medical records will be retained for at least ten (10) years from the last treatment date.” (*ADM 1.72 Record Retention, Disposal and Archiving*)

- D. Destruction/disposal shall be suspended for records involved in any open investigation, including research misconduct, audit or litigation.
- E. Paper documentation containing PHI must be shredded or placed in a secure bin. Protected Health Information must not be discarded in trash cans, unsecured recycle bins or other areas accessible by the public.
- F. The IU HIPAA Affected Area must ensure proper destruction/disposal methods by developing a procedure that meets the needs, security, and confidentiality of its area and which does not permit recovery, reconstruction or future use of the protected information.

The method of destruction/disposal for a particular type of record must be appropriate to the medium. In general, examples of proper disposal methods may include, but are not limited to:

- **Paper Records:** shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
  - **Electronic Media:** securely wiping (*using software or hardware products to overwrite media with non-sensitive data*), purging (*degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains*), or destroying the media (*disintegration, pulverization, melting, incinerating, or shredding*).
- G. UITS or the IT support personnel for the IU HIPAA Affected Area should be contacted to coordinate the destruction of any electronic media containing ePHI.
  - H. Outside vendors providing destruction and disposal services must be approved by IU's Purchasing department. To ensure the contract meets the requirements of the HIPAA Privacy and Security Rules, a Business Associate Agreement must be executed and the vendor may be required to go through a security risk assessment.

### III. Documentation of Destruction/Disposal of PHI:

Destruction of records maintained as part of the designated record set or as required by contractual agreement must be documented and the documentation maintained permanently by the IU HIPAA Affected Area (*see the sample Certificate of Destruction form attached to this policy*). Permanent retention is required because it may become necessary to demonstrate that the records were destroyed/disposed of in the regular course of business.

Records of destruction/disposal should include:

- Date of destruction;
- Method of destruction;
- Description of the destroyed documents;
- Inclusive dates covered;
- Statement that the records were destroyed in the normal course of business; and
- Signatures of the individuals supervising and witnessing the destruction.
- Destruction documents should be permanently retained by the Unit Privacy Officer, or the University Privacy Officer, as applicable; and
- Name of IU approved vendor, if applicable.

### IV. Violations:

- A. The IU HIPAA Affected Area must report any violation of this policy and/or unintentional destruction of PHI to the University HIPAA Privacy Officer.

- B. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation.
- C. Failure to comply with this policy can result in significant consequences to the individual as well as Indiana University, including violations of law, investigations, and criminal proceedings. Accordingly, individuals who violate this policy may be subject to a full range of sanctions, including disciplinary action, suspension, termination of employment and legal action.

---

## Sanctions

HIPAA-G01 – HIPAA Sanctions Guidance

---

## Appendix

Appendix 1 – Certificate of Destruction

---

## Related Information

### Indiana Code

Indiana Code § 16-39-7-1: Maintenance of health records by providers; Violations

### HIPAA Privacy Rule

45 CFR 164.530I

45 CFR 164.530(e)

### HIPAA Security Rule

45 CFR 164.310

45 CFR 164.310(d)(2)(i) and (ii)

### Related IU Policies/Guidance Documents

HIPAA-G01: HIPAA Sanctions Guidance

---

## History

07/01/2015	Effective Date
08/01/2016	Added link for Glossary
06/xx/2017	Published on University policy site

# Appendix 1



## INDIANA UNIVERSITY CERTIFICATE OF DESTRUCTION

The information described below was destroyed in the normal course of business pursuant to Indiana University's retention schedule and destruction policy and procedures.

Date of Destruction: \_\_\_\_\_ Authorized By: \_\_\_\_\_

Description of the Information Destroyed/Disposed of:

---

---

Dates Covered: \_\_\_\_\_

---

### TYPE OF RECORD:

- Paper
- Electronic
- Both

### METHOD OF DESTRUCTION:

#### ***If Paper:***

- Shredding
- Burning
- Pulping
- Pulverizing
- Other: \_\_\_\_\_

#### ***If Electronic:***

- Secure Wiping/Overwriting
- Reformatting
- Other: \_\_\_\_\_

---

Records Destroyed By: \_\_\_\_\_

Witnessed By: \_\_\_\_\_

Department/Unit Manager: \_\_\_\_\_

*\*If records are destroyed by a vendor, the IU HIPAA Affected Area must use an IU approved vendor.*

---

***Retain Certificate of Destruction permanently***