# JOHNS HOPKINS PERSONALLY IDENTIFIABLE INFORMATION POLICY

## Application of Policy

The Johns Hopkins Personally Identifiable Information Policy ("PII Policy") sets forth the minimum standards for the Johns Hopkins University ("JHU" or the "University" ) and the Johns Hopkins Health System Corporation ("JHHS") (JHU and JHHS are "Hopkins" or "Johns Hopkins") to protect personally identifiable information ("PII"). These standards are cast as practices herein; they represent the set of expectations against which policy compliance will be assessed. Further obligations imposed by law, regulations, contract or other institutional policies also apply.

All members of the Hopkins community, including without limitation, Hopkins students, faculty, staff, employees, volunteers and contractors, are required to adhere to this PII Policy.

## Policy

It is Johns Hopkins policy to protect the privacy of personally identifiable information that is within Hopkins' control. PII is information that can be used to identify an individual, whether on its own or in combination with other personal or identifying information that is linked or linkable to an individual. PII can be that of current and prospective workforce members, students, alumni, donors, trustees, advisory committee members, vendors, visitors, and payors, among others. Privacy requirements regarding minors may require additional consideration regarding information classification and/or handling.

Protected health information (PHI) is governed under the federal HIPAA law (see below) and Hopkins has a comprehensive set of policies, standards and practices for this law. It is therefore not governed under this policy. PII of patients, clinical research study subjects and workforce members as health plan participants constitutes PHI.

Federal and state information privacy laws require Hopkins to protect certain elements of PII, often because of the sensitivity of the data and/or its potential for misuse for fraudulent activities or other forms of identity theft. These laws may require Hopkins to self-report to the state or federal government and/or provide notice to affected individuals if the security of certain PII is breached.

The following table provides examples of different types of PII:

| Examples of PII that may require legal notification of breach | Examples of Other Legally Protected PII that is considered Sensitive/Confidential | Examples of Other Forms of PII with the potential for misuse |
|---|---|---|
| Social Security numbers | Student Education Records | Date of Birth |
| Credit card numbers | Grades, Transcripts, Schedules | User credentials |
| Financial account information | Banking and personal financial information related to student financial aid that does not include account information (e.g. credit scores) | Partially redacted PII (e.g., last 4 digits of SSN) |
| Driver's license numbers | Employee records (e.g. human resources) | Employee ID numbers |
| | Records of administrative hearing | |

A given element of PII may be protected under more than one federal or state law or Hopkins policy. Hopkins has adopted other information privacy policies governing specific categories of information, as set forth in the next section. The third column above includes PII that is sensitive but may be an appropriate substitute for other legally protected PII elements.

The PII elements below are not necessarily considered private, but combining these elements with other PII may have privacy implications.

| Examples of Other PII that may be misused if combined with other PII or aggregated |
|---|
| Address |
| Phone number |
| Email address |
| JHED ID |
| Student directory information in which the student has not opted out (like that above, but also dates and photos) |

## Hopkins Information Privacy Policies

If any specific Hopkins policy, including without limitation the ones listed below, conflict with this general privacy policy, that policy will control.

1. Student Records -- The Johns Hopkins University Policy on Family Educational Rights and Privacy (http://pages.jh.edu/~news_info/policy/ferpa.html) addresses student privacy rights with respect to their education records, as required under the federal Family Educational Rights and Privacy Act ("FERPA"). The Hopkins Registrars have primary responsibility for establishing policies and procedures related to compliance with FERPA.

2. Electronic Information that is Restricted, Confidential or Internal-Use-Only -- Hopkins requires protection, in compliance with the Hopkins information technology policies

(http://it.jhu.edu/policies/itpolicies.html), of electronic information that is categorized as restricted, confidential or internal-use-only.

3. Health Information of Patients, Health Information of Health Plan Members and Health Information of Human Subjects Participating in Clinical Research with a Covered Entity -- The confidentiality of patients, clinical research study subjects and health plan members information is covered under separate Johns Hopkins Medicine policies addressing protected health information (HIPAA Provider policy available at https://hpo.johnshopkins.edu/enterprise/policies/170/12134/policy_12134.pdf?_=0.950377349296 and HIPAA Health Plan policy available at https://hpo.johnshopkins.edu/enterprise/policies/181/12226/policy_12226.pdf?_=0.277344938423), and is thus not addressed in this policy. The Hopkins Privacy Office has primary responsibility for establishing policies and procedures related to compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") for the relevant divisions of Hopkins.

4. Human Subjects Research -- In addition to HIPAA and other laws safeguarding the privacy of health information, the Federal Policy for the Protection of Human Subjects (the "Common Rule") contains protections for the privacy of research participants and the confidentiality of their information. Confidentiality and privacy with respect to non-medical human subjects research is addressed by the appropriate JHU divisional Institutional Review Board ("IRB") policies and procedures.

5. Identity Theft Prevention Policy -- The U.S. Federal Trade Commission requires organizations that routinely deal with consumer accounts to maintain a policy regarding "red flags" that might indicate consumer identity theft. While these flags may not involve PII, unusual account activity may be an indicatory for detection. http://pages.jh.edu/~news_info/policy/identity_theft.html

**Protection and Handling of PII**

The following requirements apply to PII in paper records, electronic records and in oral communications, as well as any aggregation of PII in an electronic format (e.g., databases, webpages, e-mail, spreadsheets, tables and file sharing services such as JHBox, Sharepoint).

1. General -- In addition to complying with all applicable legal requirements, Hopkins further limits the collection, use, disclosure, transmission, storage and/or disposal of PII to that which fulfills the Johns Hopkins mission.

2. Safeguards -- To protect PII against inappropriate access, use, disclosure, or transmission, Hopkins requires appropriate administrative, technical and physical safeguards. Divisional and entity leadership is responsible for documenting security controls and safeguards and risk management consistent with the Hopkins policy. Examples of physical safeguards include storing documents containing PII in secured

cabinets or rooms and ensuring that documents containing PII are not left on desks or in other locations that may be visible to individuals not authorized to access the PII.

3. Collection – Collection of PII should be done in a way that is consonant with the other provisions of this section (e.g., Minimization). Collected data should be appropriate for the intended authorized use, and collection should be conducted according to best practice and legal requirements for the type and purpose of data collected. Since the collection process itself can potentially lead to unintended PII disclosure, considerations of confidentiality in collection and recording should be explicitly addressed.

4. Minimization -- All members of the Hopkins community (e.g. employees, staff, contractors and volunteers) are responsible for minimizing the use of PII (including redaction of financial account information, use of less sensitive substitutes such as partial SSN and the Hopkins Unique Identifier) and minimizing aggregations of PII. The risk of unauthorized disclosure of or access to PII increases with the amount of data. All members of the Hopkins community are responsible for ensuring that the number and scope of physical and electronic copies and repositories of PII are kept to the minimum necessary and only for the time period where a valid business need for the information exists.

5. Permitted Use within Hopkins -- Only individuals within Hopkins who are permitted under law, regulation and Hopkins policies and have a legitimate "need to know" are authorized to access, use, transmit, handle or receive PII, and that authorization only extends to the specific PII for which the relevant individual has a legitimate “need to know” for the purposes of performing his or her Hopkins job duties.

6. Permitted Disclosure to Third Parties -- Hopkins may release PII to third parties only as permitted by law/regulation and Hopkins policy. Third party contractors to whom Hopkins is disclosing PII must be bound by agreements with appropriate PII safeguarding and use provisions.

7. Oral Communications -- Only authorized individuals may engage in oral communications involving PII. Caution is required in all oral communications involving PII, and oral communications involving PII may not take place in any location where the communication may be overheard by an individual not authorized to access the PII.

8. Storage of PII -- PII may be stored only as necessary for the Johns Hopkins mission and permitted under the Hopkins policy. Divisional and Departmental leadership is responsible for providing guidelines around where information can be scanned/stored (e.g. in hardcopy, on shared drives, on other media/devices) and how long information may be retained before requiring deletion or destruction). In addition, divisional and entity leadership is responsible for maintaining an up-to-date inventory of stored or maintained documents, files, data bases and data sets containing PII, and their contents;

and requiring encryption of PII stored on mobile devices, media or other at-risk devices such as public workstations.

9. Transmission of PII -- PII may not be transmitted to external parties outside Hopkins (e.g. via mail, fax, e-mail, FTP, instant messaging) without appropriate security controls. Generally, such controls include encryption and authentication of recipients (e.g., password protection of files; verifying fax numbers; cover sheets; marking documents as confidential). Great care is to be taken to ensure that e-mails are sent only to intended recipients.

10. Disposal -- PII must be destroyed and rendered unreadable prior to disposal. For example, this may include shredding papers or wiping electronic files.

11. Training -- Each Hopkins division, entity and department is responsible for ensuring that its personnel complete appropriate training on the Hopkins information privacy policies and sign confidentiality agreements to the extent necessary and appropriate, before accessing, using, transmitting, handling or receiving PII.

**Enforcement and Exceptions**

Each Hopkins division, entity, and department is responsible for ensuring that its PII handling practices are consistent with the practices described in this PII Policy. This responsibility includes the entire set of activities within *enforcement*, including surveillance and detection of non-compliance with the Policy, the identification and implementation of individual- and organizational-level corrective actions, and (where appropriate) the imposition of sanctions. As a practical matter, it may be occasionally necessary and appropriate to diverge from these best practices in order to advance the institution's mission. In such cases, it is the responsibility of the head of the relevant division, entity, or department to ensure that such divergences are approved, documented, and communicated to stakeholders.

**Breaches of the Privacy of PII**

Known or suspected violations of this policy should be reported promptly. Any incidents that have the potential to damage departmental and/or Hopkins network operations should be reported immediately. Violators of this policy may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

In the event of a known or suspected privacy breach, contact for the University, the Office of the General Counsel, at (410) 516-8128 and for JHHS, JHHS Legal Department, 410-955-7949.

*Related Laws, Rules and Standards:*
Family Educational Rights and Privacy Act and associated regulations
Gramm-Leach-Bliley Act and the FTC's Information Safeguarding Rule

Health Insurance Portability and Accountability Act (HIPAA) and associated regulations
Health Information Technology for Economic and Clinical Health Act (HITECH) and associated regulations
Fair and Accurate Credit Transactions Act and the FTC's "Red Flags" Rule
Children's Online Privacy Protection Act
Maryland Confidentiality of Medical Records Act
Maryland Social Security Number Privacy Act
Maryland Personal Information Protection Act
Payment Card Industry Data Security Standards