	Johns Hopkins Medicine JHM Corporate and Administrative Policy Manual Administration	<i>Policy Number</i>	ADMIN019
	<i>Subject</i> Privacy and Protection of Sensitive Information	<i>Effective Date</i>	08/01/2020
		<i>Page</i>	1 of 6
		<i>Supersedes Date</i>	06/30/2020

This document applies to the following Participating Organizations:

All Children's Health System, Inc.	Howard County General Hospital	Johns Hopkins All Children's Hospital	Johns Hopkins Bayview Medical Center
Johns Hopkins Community Physicians	Johns Hopkins HealthCare LLC	Johns Hopkins Home Based Services	Johns Hopkins Medicine International
Johns Hopkins School of Medicine	Johns Hopkins Surgery Centers Series	Sibley Memorial Hospital	Suburban Hospital
The Johns Hopkins Health System Corporation	The Johns Hopkins Hospital		

Keywords: personally identifiable information, PII, protected health information, sensitive information

Table of Contents	Page Number
I. PURPOSE	1
II. POLICY	1
III. DEFINITIONS	2
IV. RESPONSIBILITIES AND PROCESS	3
V. DISSEMINATION	4
VI. SUPPORTIVE INFORMATION	4
VII. SIGNATURES	5

I. PURPOSE

This Johns Hopkins Privacy and Protection of Sensitive Information Policy (“Sensitive Information Policy”) sets forth the minimum standards for the Participating Organizations (also sometimes referred to in this Policy as “Hopkins” or “Johns Hopkins”-- all three terms meaning the organizations covered by this Policy) to protect Personally Identifiable Information (PII) and Protected Health Information (PHI). The standards set forth are cast as practices; 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.


Protected Health Information (PHI) is governed under the federal Health Insurance Portability and Accountability Act and its related regulations (HIPAA) and Hopkins has a comprehensive set of policies, standards and practices for HIPAA compliance.

Federal and state information privacy laws require Hopkins to protect certain elements of Sensitive Information, 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 Sensitive Information is breached.

II. POLICY

This policy does NOT supersede the Johns Hopkins HIPAA policies but rather supplements them; to the extent that PHI is involved and a Johns Hopkins HIPAA policy is more stringent than, or inconsistent with, this Policy, then the Johns Hopkins HIPAA policy prevails over this Policy.

Sensitive Information that is PII can be that of current and prospective workforce members, students, alumni, donors, trustees, advisory committee members, vendors, visitors, and payors, among others, when such information is about such individuals in those roles but not information of those individuals in the role of a patient, research study subject or health plan member. Privacy requirements regarding minors may require additional consideration regarding information classification and/or handling.

	Johns Hopkins Medicine JHM Corporate and Administrative Policy Manual Administration	<i>Policy Number</i>	ADMIN019
		<i>Effective Date</i>	08/01/2020
	<i>Subject</i> Privacy and Protection of Sensitive Information	<i>Page</i>	2 of 6
		<i>Supersedes Date</i>	06/30/2020

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	Dates of Birth
Credit card numbers	Grades, Transcripts, Schedules	User credentials
Financial account information	Banking and personal financial information	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 hearings	


A given element of Sensitive Information 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. 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


III. DEFINITIONS

PHI or Protected Health Information	Individually identifiable health information. Applies to information of patients, research study subjects and health plan members and anyone who may have another association with Johns Hopkins (such as a workforce member or student) when in the role of patient, research study subject or health plan member.
PII or Personally Identifiable Information	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. Does not apply to workforce members, students, donors and others who have an affiliation with Johns Hopkins when in the role of a patient, research study subject or health plan member.
Sensitive Information	PHI and PII individually and collectively.

	Johns Hopkins Medicine JHM Corporate and Administrative Policy Manual Administration	<i>Policy Number</i>	ADMIN019
	<i>Subject</i> Privacy and Protection of Sensitive Information	<i>Effective Date</i>	08/01/2020
		<i>Page</i>	3 of 6
		<i>Supersedes Date</i>	06/30/2020

IV. RESPONSIBILITIES AND PROCESS

- A. Participating Organization leadership is responsible for overseeing adherence to this policy, working through the respective privacy liaisons and with the Johns Hopkins Privacy Office.
- B. All members of the Hopkins community, including without limitation, Hopkins students, faculty, staff, employees, workforce members, interns, residents, fellows, researchers, temporary personnel, volunteers and contractors, are required to adhere to this Sensitive Information Policy.
- C. The following requirements apply to Sensitive Information in paper records, electronic records and in oral communications, as well as any aggregation of Sensitive Information in an electronic format (e.g., databases, webpages, e-mail, spreadsheets, tables and file sharing services such as JHBox).
 1. General -- In addition to complying with all applicable legal requirements, Hopkins further limits the collection, use, disclosure, transmission, storage and/or disposal of Sensitive Information to that which fulfills the Johns Hopkins mission.
 2. Safeguards -- To protect Sensitive Information 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 Sensitive Information in secured cabinets or rooms and ensuring that documents containing Sensitive Information are not left on desks or in other locations that may be visible to individuals not authorized to access the Sensitive Information.
 3. Collection -- Collection of Sensitive Information 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 Sensitive Information 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 Sensitive Information (including redaction of financial account information, use of less sensitive substitutes such as partial SSN and the Hopkins Unique Identifier (pernr)) and minimizing aggregations of Sensitive Information. The risk of unauthorized disclosure of or access to Sensitive Information 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 Sensitive Information 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 Sensitive Information, and that authorization extends only to the specific Sensitive Information 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 Sensitive Information to third parties only as permitted by law/regulation and Hopkins policy. Third party contractors to whom Hopkins is disclosing Sensitive Information must be bound by agreements with appropriate Sensitive Information safeguarding and use provisions.
 7. Oral Communications -- Only authorized individuals may engage in oral communications involving Sensitive Information. Caution is required in all oral communications involving Sensitive Information, and oral communications involving Sensitive Information may not take place in any location where the communication may be overheard by an individual not authorized to access the Sensitive Information.
 8. Storage of Sensitive Information -- Sensitive Information may be stored only as necessary for the Johns Hopkins mission and permitted under the Hopkins policy. 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, department and entity leadership is responsible for maintaining an up-to-date inventory of stored or maintained documents, files, data bases

	Johns Hopkins Medicine JHM Corporate and Administrative Policy Manual Administration	<i>Policy Number</i>	ADMIN019
	<i>Subject</i> Privacy and Protection of Sensitive Information	<i>Effective Date</i>	08/01/2020
		<i>Page</i>	4 of 6
		<i>Supersedes Date</i>	06/30/2020

and data sets containing Sensitive Information, and their contents; and requiring encryption of Sensitive Information stored on mobile devices, media or other at-risk devices such as public workstations.

9. Transmission of Sensitive Information -- Sensitive Information 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., encryption 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 -- Sensitive Information must be destroyed and rendered unreadable prior to disposal. For example, this may include shredding papers or wiping electronic files.
 11. Training -- Each Participating Organization is responsible for ensuring that its personnel complete appropriate training on the Hopkins information privacy and security policies and sign confidentiality agreements to the extent necessary and appropriate, before accessing, using, transmitting, handling or receiving Sensitive Information.
- D. Enforcement and Exceptions
1. Each Participating Organization is responsible for ensuring that its Sensitive Information handling practices are consistent with the practices described in this Sensitive Information Policy. This responsibility is for 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 occasionally may be 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 entity, department or functional unit to ensure that such divergences are approved, documented, and communicated to stakeholders.
- E. Breaches of the Privacy of Sensitive Information
1. Known or suspected violations of this Policy should be reported promptly to the Johns Hopkins Privacy Office. 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.
 2. In the event of a known or suspected privacy breach, contact the Johns Hopkins Privacy Office at 410-614-9900 or at hipaa@jhmi.edu .

V. DISSEMINATION

This policy will be communicated to the appropriate Hopkins personnel via the following channels:


1. The Privacy Liaison(s) of each Participating Organization will be accountable for dissemination and implementation of this policy.
2. Substantive updates and revisions shall be communicated at the monthly JHM Corporate and Administrative Committee policy meetings.
3. This policy shall be placed on the enterprise location of the [Hopkins Policy and Document Library website](#).

VI. SUPPORTIVE INFORMATION

See Also:

- JHM Corporate and Administrative Manual, [ADMIN020 Data Privacy and Protection Program Policy](#)
- Johns Hopkins Health System PCI Standards Compliance Policy (FIN37)
- [Johns Hopkins Privacy Office Intranet Site](#)

References:

	Johns Hopkins Medicine JHM Corporate and Administrative Policy Manual Administration	<i>Policy Number</i>	ADMIN019
	<i>Subject</i> Privacy and Protection of Sensitive Information	<i>Effective Date</i>	08/01/2020
		<i>Page</i>	5 of 6
		<i>Supersedes Date</i>	06/30/2020

Related Laws, Rules and Standards:

1. Family Educational Rights and Privacy Act and associated regulations
2. Gramm-Leach-Bliley Act and the FTC's Information Safeguarding Rule
3. Health Insurance Portability and Accountability Act (HIPAA) and associated regulations
4. Health Information Technology for Economic and Clinical Health Act (HITECH) and associated regulations
5. Fair and Accurate Credit Transactions Act and the FTC's "Red Flags" Rule
6. Children's Online Privacy Protection Act
7. Payment Card Industry (PCI) Data Security Standards
8. Various state statutes in Maryland, District of Columbia, and Florida

Sponsor:

- JHM Corporate and Administrative Policy Committee

Developer(s):

- Johns Hopkins Privacy Office


Review Cycle:

- Three (3) Years

VII. SIGNATURES

Revision history note: On 8/1/20, JHSCS was added as a participating organization.

Electronic Signature(s)	Date
Lisa Ishii President, Johns Hopkins Surgery Center; Senior Vice President, Operations, Johns Hopkins Health System	06/30/2020
Paul Rothman Dean of the Medical Faculty, Chief Executive Officer, Johns Hopkins Medicine	10/21/2016
Redonda Miller President, The Johns Hopkins Hospital	10/21/2016
Richard Bennett President, Johns Hopkins Bayview Medical Center	10/21/2016
Jacqueline Schultz President, Suburban Hospital	10/24/2016
Steven Snelgrove President, Howard County General Hospital	10/21/2016

	Johns Hopkins Medicine JHM Corporate and Administrative Policy Manual Administration	<i>Policy Number</i>	ADMIN019
		<i>Effective Date</i>	08/01/2020
	<u>Subject</u> Privacy and Protection of Sensitive Information	<i>Page</i>	6 of 6
		<i>Supersedes Date</i>	06/30/2020

Steven Kravet President, Johns Hopkins Community Physicians, Inc.	10/26/2016
Mary Myers President, Johns Hopkins Home Care Group	10/11/2019
Kevin Sowers President, Johns Hopkins Health System Corporation	10/09/2019
Hasan Zia (CL) President, Sibley Memorial Hospital	10/09/2019
James Holland President, Johns Hopkins HealthCare LLC	10/09/2019
Charles Wiener President, Johns Hopkins Medicine International	10/09/2019
Thomas Kmetz Interim President, Johns Hopkins All Children's Hospital and Health System	10/09/2019