A Manager’s Guide: Patient Privacy at Johns Hopkins (For Providers)

The Johns Hopkins Privacy Office
5801 Smith Avenue
McAuley Hall, Suite 310
Baltimore, MD 21209
(410) 735-6509

*Note: Information found in this guide relates ONLY to the Johns Hopkins activities in the United States of America.

This document is intended to be accessed electronically. To access the most current version of this guide, visit: http://intranet.insidehopkinsmedicine.org/privacy_office/docs/additional_information/managers_guide_to_patient_privacy.pdf
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Regulatory Overview</td>
<td>3</td>
</tr>
<tr>
<td>Contact Information</td>
<td>4</td>
</tr>
<tr>
<td>Commonly Used Terms</td>
<td>5</td>
</tr>
<tr>
<td>Training</td>
<td>7</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>9</td>
</tr>
<tr>
<td>Patient Rights</td>
<td>11</td>
</tr>
<tr>
<td>Breach Events</td>
<td>13</td>
</tr>
<tr>
<td>Subpoenas, Court or Administrative Orders Seeking/Requesting PHI</td>
<td>14</td>
</tr>
<tr>
<td>Requests to Disclose or Release PHI/Medical Records</td>
<td>16</td>
</tr>
<tr>
<td>Common Uses and Disclosures of PHI</td>
<td>18</td>
</tr>
<tr>
<td>• Treatment, Payment and Health Care Operations</td>
<td></td>
</tr>
<tr>
<td>• Involved in a Patient’s Care</td>
<td></td>
</tr>
<tr>
<td>• Decedents</td>
<td></td>
</tr>
<tr>
<td>• Required by Law</td>
<td></td>
</tr>
<tr>
<td>• Law Enforcement</td>
<td></td>
</tr>
<tr>
<td>• Public Health</td>
<td></td>
</tr>
<tr>
<td>• Health Oversight Activities</td>
<td></td>
</tr>
<tr>
<td>HIPAA Related Agreements</td>
<td>20</td>
</tr>
<tr>
<td>Quick Reference Key Guidance Topics</td>
<td>Appendix A</td>
</tr>
<tr>
<td>• Minimum Necessary</td>
<td></td>
</tr>
<tr>
<td>• Electronic Communications</td>
<td></td>
</tr>
<tr>
<td>• Faxing and Mailing PHI</td>
<td></td>
</tr>
<tr>
<td>• Social Media/Networking</td>
<td></td>
</tr>
<tr>
<td>• Portable Electronic Devices</td>
<td></td>
</tr>
<tr>
<td>• Taking PHI Off-Site</td>
<td></td>
</tr>
<tr>
<td>Quick Reference – Key Privacy Policies and Forms</td>
<td>Appendix B</td>
</tr>
<tr>
<td>Checklist for Privacy Compliance Tool</td>
<td>Appendix C</td>
</tr>
</tbody>
</table>
Introduction

This reference guide is designed to give Johns Hopkins managers/supervisors a brief overview of how Johns Hopkins has implemented the HIPAA regulations and other applicable laws.

---

It is the policy of Johns Hopkins (JH) to protect the privacy and security of all patients, health plan members, employees, students and donors; to maintain the confidentiality of patient information and to comply with all applicable laws and regulations, including the Privacy Regulations under HIPAA. Keeping patient information private and secure is an integral part of providing good customer service to our patients and aids in maintaining their trust and respect.

As a manager/supervisor within a JH organization that is subject to HIPAA (a “covered entity”), it is important to understand that responsibility for compliance with all applicable laws and regulations, including HIPAA and the related JH policies and procedures lies with management of the various JH covered entities.

Johns Hopkins Privacy Office

JH has a centralized Privacy Office. The mission of the Privacy Office is to encourage and assist JH covered entities in complying with the HIPAA privacy regulations, other applicable federal and state privacy laws, and related Johns Hopkins HIPAA policies and procedures. The Privacy Office provides direction and advice over all Johns Hopkins HIPAA covered entities and functions, for both the Health System and the University, for both providers and for health plans.

Johns Hopkins Privacy Officer and Chief Information Security Officer

There is only one Privacy Officer and one Chief Information Security Officer for all HIPAA covered entities and functions within Johns Hopkins (with the exception of All Children’s Hospital and its related entities). All privacy complaints, requests to amend health information, requests for an accounting of disclosures of health information, as well as all communications from the U.S. Department of Health & Human Services Office for Civil Rights, or any other regulatory or enforcement agencies relating to privacy and HIPAA, are to be referred to JH Privacy Office.

Privacy Office Intranet

The Privacy Office maintains a comprehensive intranet site that can be accessed by JH workforce members. The intranet site contains a wealth of information about the HIPAA regulations and how they have been implemented at JH. All JH privacy policies and related forms can be accessed through the Privacy Office intranet site. In addition, all privacy related requests, questions and concerns may be submitted through the intranet site. To access the Privacy Office intranet site, visit: http://intranet.insidehopkinsmedicine.org/privacy_office/index.html.

HIPAA Related Forms and Policies

All HIPAA related forms and policies available on the Privacy Office intranet site are “owned” by the Privacy Office and are not to be modified. To the extent your department/clinic/business area needs a unique form for HIPAA purposes, contact the Privacy Office. Forms may be downloaded from the Privacy Office intranet site at: http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/find_a_form.html. Alternatively, your department has the option of ordering some forms in bulk from Standard Register using the following steps:

---

1 Refer to page #4 of this guide for contact information.
- For **Johns Hopkins Health System** departments: use Standard Register’s *SMARTworks* system
- For **Johns Hopkins University** departments: use the *SAP* system

If you do not have access to either of these systems, please contact the Johns Hopkins account team at Standard Register at toccsc.eh2@standardregister.com. There are various account team members who manage the e-mail account; therefore, e-mail is the most effective and quickest way for the account team to respond to questions. Standard Register does not offer paper order forms. JHHS departments may request access to the Standard Register’s SMARTworks system by sending the following information to the above email address: cost center number, and the name/email/phone number of the individual for whom access is requested. If you need further assistance, Mike Hennessie is the Standard Register contact onsite at Johns Hopkins (phone 410-276-6145 and email mike.hennessie@standardregister.com).
Regulatory Overview

HIPAA

"HIPAA" is the acronym for the federal legislation titled Health Insurance Portability and Accountability Act of 1996. The main purposes of this federal statute were (i) to help consumers maintain their insurance coverage as they changed employers and (ii) to lay the groundwork for the electronic exchange of health information. Because of the latter goal, HIPAA also includes a separate set of provisions called “Administrative Simplification.” The key components of Administrative Simplification include: Privacy and Security standards to protect the confidentiality of protected health information (PHI), Transaction and Code Sets, the National Provider Identifier requirements, and the National Health Plan Identifier requirements. HIPAA applies to Health Plans, Health Care Clearinghouses, Health Care Providers (who transmit electronic transactions covered by the HIPAA regulations) and Medicare Part D Pharmaceutical Providers. Collectively, they are known as “covered entities.” The Privacy and Security Standards apply to individually identifiable health information held or used by covered entities referred to as “Protected Health Information” or “PHI.”

I. Privacy Rule

The Privacy Rule set national standards for the protection of health information, as applied to covered entities\(^2\). Under this Rule, covered entities are required to have in place standards to protect and guard against the misuse of PHI. The Privacy Rule also granted patients certain individual rights with respect to the use and disclosure of their PHI:

1. Right to a notice of privacy practices
2. Right to obtain access to their own health record
3. Right to obtain an accounting of disclosures
4. Right to request restrictions and confidential communications concerning protected health information
5. Right to request amendment of protected health information
6. Right to be notified in the event of a breach of PHI

II. Security Rule

The HIPAA security regulations, implemented on April 21, 2005, established standards for the security of electronic PHI (e-PHI). Those standards include Administrative Safeguards, Physical Safeguards and Technical Safeguards for maintaining the confidentiality and integrity of e-PHI. The Security Rule specifies technical and non-technical safeguards that covered entities must have in place to secure e-PHI.

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act is part of the American Recovery and Reinvestment Act of 2009. Due to the anticipated expansion in the exchange of e-PHI, the HITECH Act widened the scope of privacy and security protections under HIPAA; increased the potential legal liability for non-compliance; and provided for greater enforcement of HIPAA.

To learn more about HIPAA, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/about_hipaa/
http://intranet.insidehopkinsmedicine.org/privacy_office/about_hipaa/history.html

\(^2\) All of the organizations within the Johns Hopkins Health System, as well as the Johns Hopkins University School of Medicine and the School of Nursing, are covered entities.

Johns Hopkins Privacy Office
Copyright © 2015
Contact the Privacy Office

For general privacy related matters, questions and/or advice:
Main: hipaa@jhmi.edu / Ph: (410) 735-6509 / Fax: (410) 735-6521

---

To submit specific requests/information to the Privacy Office:
Subpoenas: subpoenas-HIPAA@jhmi.edu / Ph: (410) 735-6504 / Fax: (410) 735-6520
Breach Events: hipaabreaches@jhmi.edu / Ph: (410) 735-6509 / Fax: (410) 735-6521
Privacy Complaints: hipaa@jhmi.edu / Ph: (410) 735-6509 / Fax: (410) 735-6521
Request an Amendment: hipaa@jhmi.edu / Ph: (410) 735-6509 / Fax: (410) 735-6521

---

Privacy Office Staff:
Donald L. Bradfield, Senior Counsel, HIPAA / dbradfi4@jhmi.edu / Ph: (410) 735-6502
Pamela S. Rayne, Associate Counsel, HIPAA / prayne1@jhmi.edu / Ph: (410) 735-7607
Carol M. Richardson, Privacy Officer / crichar6@jhmi.edu / Ph: (410) 735-6544
Teresa R. Burns, Deputy Privacy Officer / tburns7@jhmi.edu / Ph: (410) 735-6518
Michelle N. Purnell, Regional Deputy Privacy Officer / mpurnel1@jhmi.edu / Ph: (410) 735-6511
Mary Valentine, HIPAA Operations Coordinator / mvalent8@jhmi.edu / Ph: (410) 735-6508
Melanie Torain, Paralegal / mtorain1@jhmi.edu / Ph: (410) 735-6504
Heather Arthur, Purnell, HIPAA Compliance Coordinator / harthur1@jhmi.edu / Ph: (410) 735-4166
Kate Denton, Privacy Compliance Analyst, HIPAA / klinebe2@jhmi.edu / Ph: (410) 735-6632
Viki Marzetti, Legal Secretary, HIPAA / vmarzet1@jhmi.edu / Ph: (410)735-6503
Jennifer Kulynych, IRB Counsel / jkulyny1@jhmi.edu / Ph: (410) 955-6514

Contact the Chief Information Security Officer

Darren Lacey, Chief Information Security Officer / dll@jhu.edu / Ph: (410) 735-4477
Commonly Used Terms

Authorization
An individual's (patient's) signed written permission to allow healthcare professionals to use or disclose his/her health information for reasons generally not related to treatment, payment or health care operations

Business Associate
A non-Johns Hopkins individual or company that uses Johns Hopkins PHI to provide a service to Johns Hopkins or to perform or do some activity on behalf of Johns Hopkins, such as consulting, legal, quality or performance review, software maintenance, mail house services, data review or aggregation or similar activities

Covered Entity
Those who must comply with HIPAA, such as:

- Health Plans (self-insured/insured, HMOs, health insurance companies, employer health plans, and similar arrangements)
- Health Care Providers (who transmit electronic transactions covered by the HIPAA regulations)
- Health Care Clearinghouses
- Medicare Part D Pharmaceutical Providers

Designated Record Set (or “DRS”)
A group of records that are maintained by or for a Johns Hopkins covered entity, that is

- the medical records and billing records of an individual maintained by or for a Johns Hopkins health care provider; or
- used, in whole or in part, by or for a Johns Hopkins covered entity to make decisions about individuals

Disclosure/Disclose
The release, transfer, provision of access to, or the divulging in any manner of PHI to persons or entities outside of the Johns Hopkins covered entities

Health Care Operations
Activities performed by a health care provider such as conducting routine business activities, providing training programs, evaluating practitioner performance, etc., that are not directly related to a patient's care or payment activities

HIPAA
HIPAA means the Health Insurance Portability and Accountability Act of 1996, and its related regulations, as amended

HITECH
HITECH means The Health Information Technology for Economic and Clinical Health Act

Individual
Individual means the person who is the subject of the PHI (e.g., a patient)
OCR
OCR means the federal Office for Civil Rights; OCR is responsible for enforcement of the HIPAA regulations

Patient Representative
A person authorized (under State or other applicable law) to act on behalf of the individual in making health care related decisions

Payment
Activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care and related activities such as determinations of eligibility or coverage, risk adjusting, billing, claims management, review of medical necessity and appropriateness of care, utilization review and pre-authorization of services

Protected Health Information (PHI)
Individually identifiable health information, including demographic information that identifies a patient, and relates to the past, present or future treatment or condition of that patient or the past, present or future payment for health care to an individual and that is received or held by Johns Hopkins

Provider
A medical professional (doctor, nurse, pharmacist, etc.) who provides medical or health services or who bills or is paid for health care in the normal course of business; also, a location (hospital, doctor's office, etc.) or company (for example, Johns Hopkins Community Physicians) that provides or bills for health care services

Treatment
The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another

Use
The sharing of, reviewing of or looking at patient information that stays within Johns Hopkins, meaning that the information is not distributed to, shared with or made available to anyone who is not a Johns Hopkins workforce member

Workforce members
Persons under the direct control of Johns Hopkins, including, but not limited to, employees, students, interns, residents, fellows, researchers, staff, faculty, volunteers and temporary personnel

For additional terms and definitions, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/additional_information/glossary.html
Training

Training Courses

All Johns Hopkins workforce members who may have access to patients or any patient information are required to take HIPAA training **within 30 days of employment or starting work.**

After initial training, each workforce member is responsible for completing a refresher course every **two years or more frequently** as directed by their manager.

In the event a workforce member is promoted or changes job functions, additional HIPAA training might be required based on the responsibilities of the new position.

A table is available on the Privacy Office intranet site to help determine which online course(s) your workforce members are required to complete: [http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/learn_what_training_you_need.html](http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/learn_what_training_you_need.html).

The **HIPAA Online Training Instructions** provide step-by-step information for accessing and completing the online courses.

**View of training course table:**

![Training Course Table]

**Note:** Management will determine the proper course(s) to be taken based on job responsibilities. When the course is completed, the manager should be provided with a copy of the training certificate to be held in the departmental personnel file. Managers may request the ability to run training reports in the MyLearning system by sending an e-mail request to **elearn@jhmi.edu**.

**To access the full online training course table and for additional information about the JH HIPAA training requirements, visit:**

* [http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/learn_what_training_you_need.html](http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/learn_what_training_you_need.html)
* [https://hpo.johnshopkins.edu/enterprise/policies/170/12207/policy_12207.pdf?_=0.561327616538](https://hpo.johnshopkins.edu/enterprise/policies/170/12207/policy_12207.pdf?_=0.561327616538)
Confidentiality Agreements

All workforce members are required to sign the Johns Hopkins Confidentiality Agreement for Workforce Members--General as a condition of work or study. By signing that Agreement, all workforce members understand that confidential information is not to be used, disclosed or discussed with others, except as allowed by policy, state and federal laws and patient authorizations. Failure to abide by the provisions of the Confidentiality Agreement may result in disciplinary action. Workforce members should sign the Confidentiality Agreement through the applicable Johns Hopkins orientation process and a copy of the signed Confidentiality Agreement should be retained in the personnel record.

To access the Johns Hopkins Confidentiality Agreement for Workforce Members - General, visit: http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_forms/A_3_1_a_Providers_Confidentiality_Agreement_Workforce.pdf

View of Confidentiality Agreement:

![Confidentiality Agreement](http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_forms/A_3_1_a_Providers_Confidentiality_Agreement_Workforce.pdf)

Note: There are other JH Confidentiality Agreements for other situations -- vendors and contractors, students, visitors and trustees. To access other JH Confidentiality Agreements, visit: Confidentiality Agreements - http://intranet.insidehopkinsmedicine.org/privacy_office/policies_and_forms_for_providers/general_forms.html.

For additional information about JH Confidentiality Agreements, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12148/policy_12148.pdf?_=0.316309605686

http://intranet.insidehopkinsmedicine.org/privacy_office/policies_and_forms_for_providers/policies.html
Notice of Privacy Practices (NPP)

Johns Hopkins has developed and distributed a standard Notice of Privacy Practices (NPP) that provides a clear explanation of the ways in which we may use and disclose a patient’s health information. The JH NPP also describes patient’s rights as well as our obligations regarding the use and disclosure of his/her health information. The notice is intended to focus patients on privacy issues and concerns, and to prompt them to have discussions with their health care providers and exercise their rights.

It is the policy of JH that a copy of the JH NPP\(^3\) will be given to every patient no later than the date of the first clinical encounter. In emergency situations, the Notice will be given as soon as reasonably practical after the emergency. The Notice is required to be offered to the patient only at the patient’s first visit. The JH NPP should also be posted\(^4\) in a prominent location within patient service areas and copies of the JH NPP should be available for patients to take.

**View of the JH NPP:**

![Notice of Privacy Practices for Health Care Providers](image)

In addition, all patients must be asked to sign a paper acknowledging the receipt of the Notice (“Acknowledgement of Receipt of Notice of Privacy Practices”) at their first visit.

If a patient refuses to sign the Acknowledgement, a “Refusal to Sign the Acknowledgement of Receipt of Notice of Privacy Practices” will be included in the medical record.

A copy of the Acknowledgement or the Refusal should be stored in the centralized medical record. If your electronic medical records system has the ability to track this information, activate the flag when the NPP is provided and the Acknowledgment is received or refused (i.e. requiring the Johns Hopkins Workforce Member to electronically document the refusal to sign instead of using the paper refusal form).

---

\(^3\) Copies of the JH NPP can be ordered from Standard Register.

\(^4\) An 11 x 17 poster is available to be ordered from Standard Register, at the expense of the Privacy Office, for display in your area to satisfy this requirement.
View of NPP Acknowledgement:

![NPP Acknowledgement Image]

http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_b_Providers_Acknowledgment_Receipt_NPP.pdf

View of NPP Refusal:

![NPP Refusal Image]

http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_c_Providers_Refusal_Sign_Acknowledgment_Receipt_NPP.pdf

---

For additional information about the JH NPP, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12137/policy_12137.pdf?_=0.205934961466

To order a poster and/or copies of the JH NPP, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/additional_information/order_forms.html

To access the JH NPP in other languages, visit:
http://www.hopkinsmedicine.org/international/patients/privacy.html
Patient Rights

Privacy Complaints
A patient has the right to complain about the misuse or inappropriate release of his/her health information. Many patients will use the terminology "my privacy has been violated," prompting the necessity to investigate why or how that may have occurred. The Privacy Office is responsible for investigating these complaints from patients.

If a patient at Hopkins wishes to file a complaint with the Privacy Office or for additional information regarding privacy complaints, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/submit_a_complaint.html.

Request to Amend a Health Record
A patient has the right to request a change to or amendment of his/her health record. Johns Hopkins either may agree to the requested amendment or, in certain circumstances, reject the requested amendment with an explanation of why the amendment was rejected.

If a patient wishes to request a change to or amendment of his/her health record, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/request_an_amendment_to_a_health_record.html.

Patient Access to Own Health Record
A patient has the right to view and/or obtain a copy of his/her health record, with the exception of the following: PHI that is not in a designated record set; psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and PHI access to which is prohibited by law.

If a patient wants to view and/or obtain copies of his/her health record, ask the patient to submit his/her request in writing using the following form: Authorization for Release of Health Information.
For additional information, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12169/policy_12169.pdf?_=0.750277695646.

Accounting of Disclosures
A patient has the right to request an accounting of disclosures JH has made of his/her health information in the six years prior to his/her request. If a patient requests an accounting, ask the patient to complete a “Request for An Accounting of Disclosures of My Protected Health Information” form and promptly submit the completed form to the Privacy Office for coordinating and overseeing the response to the request: Request for an Accounting of Disclosures of My Protected Health Information.
For additional information, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12171/policy_12171.pdf?_=0.0595350315232.

Restriction Requests
A patient has the right to ask that his/her health information not be given to or shared with certain other individuals or agencies under certain circumstances. Johns Hopkins will agree only to five specific restrictions on the disclosure of PHI.

To learn more about those five restrictions, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12168/policy_12168.pdf?_=0.600869528312.
Confidential Communications
A patient has the right to request that we communicate with him/her about his/her health information in a certain way or at a certain location. If a patient requests that we communicate with him/her in particular way, he/she must submit that request in writing along with specification of an alternative address or other method of contact.

For additional information, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12168/policy_12168.pdf?_=0.600869528312.

Breach Notification
A patient has the right to be notified if his/her medical information has been “breached”. See the “Breach Events” section of this reference guide for additional information or visit:

For additional policies and forms, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/policies_and_forms_for_providers/policies.html
http://intranet.insidehopkinsmedicine.org/privacy_office/policies_and_forms_for_providers/authorizations.html
http://intranet.insidehopkinsmedicine.org/privacy_office/policies_and_forms_for_providers/general_forms.html
Breach Events

A HIPAA breach event is any use or disclosure of protected health information (PHI) that is, or may be, in violation of HIPAA privacy requirements.

Common examples of breach events are:

- A patient’s record is mailed, faxed or handed to the wrong person.
- A patient’s electronic record is accessed when there is no job-related need to access it and prior written permission was not received from the Privacy Office, whether the access was intentional or accidental.

Check the exclusions (see "What are the exclusions that do not need to be reported?") to ensure that the event needs to be reported. If reporting is required, fill out the Breach of Privacy or Security of PHI Event Questionnaire to provide the Privacy Office with details of the event.

View of questionnaire:

Email the completed questionnaire and all related documentation to hipaabreaches@jhmi.edu. If you are unable to e-mail the information, fax the information to 410-735-6521 using a fax cover sheet (Fax Transmittal Cover Sheet Template). Send the fax to the attention of “HIPAA Breaches.”

The Privacy Office will review the submitted information and may ask the person who reported the breach event to supply additional information. During its review, the Privacy Office will determine if the patient’s information has been “compromised” and decide if a formal notification will be sent to the patient. In addition, the person who reported the event will be notified by email with an explanation the outcome of the review.

For additional information about breach events or to report a breach, visit: http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/report_a_breach_event.html.
Subpoenas, Court or Administrative Orders Seeking/Requesting PHI

Except as noted below, copies of all subpoenas for Protected Health Information (for records or testimony), together with copies of any accompanying items (letters, certificates of service, etc.) received by every Johns Hopkins covered entity or department or center within a covered entity must be forwarded immediately upon receipt to the Johns Hopkins Privacy Office (part of the Legal Department) via email (subpoenas-hipaa@jhmi.edu) or fax (410-735-6520). If you fax subpoenas to the Privacy Office, please include a fax cover sheet with contact information for identification purposes, so the Privacy Office will know where to send instructions.

No action on such requests should be taken until the Privacy Office has provided guidance.

Once review has been completed, the Privacy Office will communicate its instructions back to the original sender of the request. Any disclosure of PHI made in response to an approved request must be tracked for purposes of accounting for disclosures.

Exceptions:

- JHH, BMC, HCGH, Suburban, Sibley, and All Children’s Hospital should send all subpoenas to their corresponding HIM (medical records) Departments.
- Johns Hopkins Community Physicians (JHCP) locations should send all subpoenas to JHCP Wyman Park HIM (medical records) Department.
- Johns Hopkins Healthcare (JHHC) should send all subpoenas to JHHC Compliance.
- JHUSOM clinics on the Bayview campus that use Meditech should forward subpoenas to BMC HIM (medical records); otherwise, JHUSOM clinics should send all subpoenas to JHH HIM (medical records) Department at 443-873-5029.

View of subpoena instruction sheet:

For additional information or to submit a subpoena for review, visit:
**Note:** Authorizations requesting PHI that are not accompanied by a subpoena should **not** be sent to the Privacy Office for review. Authorizations not accompanied by a subpoena may be reviewed for compliance by your staff using the following checklist: http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_forms/A_2_1_1_Providers_Checklist_Authorization_From_Third_Party.pdf.
Requests to Disclose or Release PHI/Medical Records

Unless a specific exception under the HIPAA regulations applies, a covered entity must obtain an individual’s written authorization to use or disclose PHI for any reason other than treatment, payment and health care operations.

Some examples of the types of things for which a covered entity would be required to obtain a specific, HIPAA compliant authorization are:

- Providing health information to a third party (other than for treatment, payment or health care operations), such as a relative, an employer (subject to exception in certain workers’ compensation contexts and certain payment contexts), or a lawyer.
- Advertisements or articles using any PHI related to the individual.

View of representative JH provider Authorization:

To find a Johns Hopkins Authorization, visit: http://intranet.insidehopkinsmedicine.org/privacy_office/policies_and_forms_for_providers/authorizations.html.

For additional information about authorizations, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12140/policy_12140.pdf?_=0.564108234083
Non-Johns Hopkins Authorizations

When you receive an Authorization for release of PHI that is not on a Johns Hopkins form, you need to review it for compliance with applicable law, before releasing the requested PHI. You may disclose the requested information only if the Authorization form includes all of the elements required by applicable law.

To determine if the form includes all of the necessary elements, use the checklist found here: http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_forms/A_2_1_1_Providers_Checklist_Authorization_From_Third_Party.pdf.

Sample generic non-JH authorization form:

For additional information about reviewing non-JH authorizations, visit: http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/review_authorizations.html.
Common Uses and Disclosures of PHI

Treatment, Payment and Health Care Operations (TPO)
In general, Johns Hopkins may use and/or disclose PHI, without authorization, for activities that fall into the following categories:

- **Treatment** – provision, coordination and management of a patient’s health care among health care providers, irrespective of whether or not the providers are Johns Hopkins providers (e.g. referral of a patient from one health care provider to another)

- **Payment** - activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care and related activities such as determinations of eligibility or coverage, risk adjusting, billing, claims management, review of medical necessity and appropriateness of care, utilization review and pre-authorization of services

- **Health Care Operations** - internal administrative, financial, legal, and quality improvement activities of a covered entity (e.g. conduct of quality assessment and improvement activities)

For more information about TPO, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12205/policy_12205.pdf?_t=0.0861176825688.

Involved in a Patient's Care
In certain circumstances, a family member or friend can be viewed as being “involved in the patient’s care.”

- If the patient is **present and able to make decisions**, "involved in the patient's care" means:
  - the patient agrees, to allow the health information to be shared; or
  - the patient could have objected to any sharing of health information, but did not; or
  - based on the circumstances, professional judgment indicates that the patient does not object to the disclosure.

- If the patient is **not present or incapacitated** (i.e. unconscious), "involved in the patient's care" means:
  - based on professional judgment, the sharing of the information is in the best interest of the patient
  - only the health information that is directly relevant to the family member's or friend's involvement should be disclosed
  - once the patient is able to make decisions, the "involvement" is determined as stated above.

It is advisable to inquire of the patient if the patient is okay with discussing his/her health information with others present or whether the patient would prefer to have the discussion in private.

For more information about “involved in a patient's care,” visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12176/policy_12176.pdf?=_t=0.00603413770951.

Decedents
Under HIPAA and state and District law, health information belonging to a deceased patient (“Decedent”) is still considered PHI and should remain private even after death. However, PHI of a decedent may be disclosed in certain circumstances.
For more information about disclosing PHI of a decedent, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/privacy_topics/decedents.html and
https://hpo.johnshopkins.edu/enterprise/policies/170/12178/policy_12178.pdf?_=0.227515782344

Required by Law
Certain Federal and State laws require Johns Hopkins to use or disclose certain PHI (e.g. reporting gunshots, stab wounds, and child or vulnerable adult abuse or neglect).
For more information about disclosures that are required by law, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12204/policy_12204.pdf?_=0.0210638510178.

Law Enforcement
Generally, PHI may not be disclosed to law enforcement officials without the patient’s authorization, except in certain instances (e.g. to locate/identify a suspect or to report a crime).
For more information about disclosures to law enforcement, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12198/policy_12198.pdf?_=0.0294755325474.

Public Health
PHI may be disclosed to a public health authority who is authorized by law to collect such information for the purposes of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.
For more information about disclosures for public health purposes, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12185/policy_12185.pdf?_=0.242096878293.

Health Oversight Activities
PHI may be disclosed to a health oversight agency for oversight activities authorized by law, such as audits related to Medicare and Medicaid and licensure activities.
For more information about disclosures for health oversight activities, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12184/policy_12184.pdf?_=0.507401411088.
HIPAA Related Agreements

Business Associate Agreements (BAA)

A BAA may be needed when an outside, non-Johns Hopkins individual or company is engaged to perform certain services for or on behalf of a Johns Hopkins health care provider, health care facility or health care plan where the outside individual or company will need access to protected health information (PHI) in order to perform its duties.

All BAAs are prepared, reviewed and maintained by the Privacy Office. Only the Johns Hopkins Medicine general counsel, or his/her designee, is authorized to sign BAAs on behalf of ANY Johns Hopkins entity.

If you believe a Business Associate Agreement (BAA) is needed (utilize the BAA Decision Tree), you must complete the form, Information Needed to Generate a BAA, and send it to the Privacy Office.

For additional information or to submit a request for a BAA, visit:
http://intranet.insidehopkinsmedicine.org/privacy_office/quick_links/request_or_review_a_business_associate_agreement.html

https://hpo.johnshopkins.edu/enterprise/policies/170/12217/policy_12217.pdf?_=0.742299532938

---

Data Use Agreements (DUA)

Johns Hopkins must enter into a data use agreement with a person or entity that is to receive a limited data set of PHI from Johns Hopkins.

All DUAs are either to be prepared by, or to be reviewed and approved/signed by, the Johns Hopkins representative involved with providing the limited data set.

When Johns Hopkins provides the limited data set, utilize the Data Use Agreement Template and review the JH HIPAA policy at:
https://hpo.johnshopkins.edu/enterprise/policies/170/12217/policy_12217.pdf?_=0.742299532938.

If any material change to the template is required or the other party's DUA is to be used, the Johns Hopkins representative must have the form reviewed by the Johns Hopkins SOM Office of Research Administration, if the project involves research; otherwise by the Johns Hopkins Privacy Office.

All DUAs are to be kept by the Johns Hopkins representative who signs the DUA for a period of 6 years from the end of their applicability.

For additional information about DUAs, visit:

https://hpo.johnshopkins.edu/enterprise/policies/170/12217/policy_12217.pdf?_=0.742299532938
Quick Reference – Key Guidance Topics

Minimum Necessary
All workforce members at all Johns Hopkins covered entities must make reasonable efforts to limit the use, disclosure of, and request for protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The minimum necessary standard applies when a Johns Hopkins covered entity, or workforce members at such covered entity, use or disclose PHI or request PHI from another covered entity.

To learn more about the minimum necessary standard, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12206/policy_12206.pdf?_=0.735246916663.

Electronic Communications
Electronic Communications are those communications that are transmitted from one person to another using an electronic medium, including e-mail, SMS, PING and text messages.

Prior to sending regular and routine Electronic Communications containing confidential information to a patient unencrypted over the internet, the risks associated with using Electronic Communications should be explained to that patient and approval obtained to use that method of communication. The Privacy Office has developed a patient consent form (Request for E-mail Communications Between Johns Hopkins Provider and Patient) that should be used when possible.

To learn more about Electronic Communications, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12164/policy_12164.pdf?_=0.681979083131.

Faxing and Mailing PHI
Fax cover sheets (Fax Transmittal Cover Sheet Template) are required when faxing documents containing PHI. You may use a fax cover sheet that you developed, but you must ensure that it contains the disclaimer clause and other required elements as noted in the fax policy template (Facsimile (Fax) Transmissions). You should be aware of other safeguards that apply to faxing and these safeguards may be found in the fax policy template found at the same site.

To learn more about faxing and mailing PHI, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12163/policy_12163.pdf?_=0.00281418964642.

Social Media/Networking
The use of social networking is becoming an increasingly popular method of communication. However, the ease of use of social networking (e.g. Facebook, Twitter, etc.) does not exempt it from ethical and legal (HIPAA) obligations regarding protecting the privacy of patients and the confidentiality of patient information.

To learn more about responsible use of Social Media/Networking, visit: https://hpo.johnshopkins.edu/enterprise/policies/170/12214/policy_12214.pdf?_=0.0372430216043.

Portable Electronic Devices
Portable electronic devices (Blackberries, Androids, iPhones, iPads, etc. = “PEDs”) have remarkable capabilities and are extremely convenient. In a healthcare setting, they make it very easy to access and share e-PHI. However, they also are easy to lose and very attractive to thieves. Therefore, PEDs should be password protected and encrypted. A password does not equate to encryption. Loss or theft of a PED containing unencrypted PHI (e.g. Ping messages, e-mails, etc.) constitutes a HIPAA “breach” of confidentially of information that triggers various reporting and formal notice obligations.
To learn more about the responsible use of PEDs and how to protect PHI, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12215/policy_12215.pdf?_=0.707059273706.

Taking PHI Off-Site

PHI, particularly original medical records, should never be taken off-site of the program or clinic location except for specific, standard and operationally necessary business purposes. “Catching up on work” is not considered a qualifying purpose. Whenever PHI can be accessed remotely using a secured connection or virtual desktop, physical PHI should not be taken off-site. The workforce member is responsible for the security of the PHI while the PHI is off-site.

To learn more about the procedures regarding taking PHI off-site, visit:
https://hpo.johnshopkins.edu/enterprise/policies/170/12216/policy_12216.pdf?_=0.327245152496.
### Quick Reference – Key Privacy Policies and Forms

<table>
<thead>
<tr>
<th>Topics</th>
<th>Quick Link to Policy</th>
<th>Quick Link to Related Form (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting of Disclosures</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12171/policy_12171.pdf?_=0.0595350315232">https://hpo.johnshopkins.edu/enterprise/policies/170/12171/policy_12171.pdf?_=0.0595350315232</a></td>
<td>[<a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_plans_forms/AB_6_4_b_Providers_Plans_Request_Accounting_Disclosures">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_plans_forms/AB_6_4_b_Providers_Plans_Request_Accounting_Disclosures</a> PHI.pdf](<a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_plans_forms)/AB_6_4_b_Providers_Plans_Request_Accounting_Disclosures">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_plans_forms)/AB_6_4_b_Providers_Plans_Request_Accounting_Disclosures</a> PHI.pdf)</td>
</tr>
<tr>
<td>Authorizations</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12140/policy_12140.pdf?_=0.564108234083">https://hpo.johnshopkins.edu/enterprise/policies/170/12140/policy_12140.pdf?_=0.564108234083</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_forms)/A_2_1_a_Providers_Authorization.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_forms/A_2_1_a_Providers_Authorization.pdf</a></td>
</tr>
<tr>
<td>Breach Notification</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12174/policy_12174.pdf?_=0.385408060494">https://hpo.johnshopkins.edu/enterprise/policies/170/12174/policy_12174.pdf?_=0.385408060494</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_plans_forms)/AB_6_6_a_Providers_Plans_Breach_Questionnaire.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_plans_forms/AB_6_6_a_Providers_Plans_Breach_Questionnaire.pdf</a></td>
</tr>
<tr>
<td>Confidentiality Agreements</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12148/policy_12148.pdf?_=0.316309605686">https://hpo.johnshopkins.edu/enterprise/policies/170/12148/policy_12148.pdf?_=0.316309605686</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_forms)/A_3_1_a_Providers_Confidentiality_Agreement_Workforce.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_forms)/A_3_1_a_Providers_Confidentiality_Agreement_Workforce.pdf</a></td>
</tr>
<tr>
<td>Decedents</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12178/policy_12178.pdf?_=0.227515782344">https://hpo.johnshopkins.edu/enterprise/policies/170/12178/policy_12178.pdf?_=0.227515782344</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_forms)/A_7_3_a_Providers_Representation_Records_of_Decedent.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms/provider_forms/A_7_3_a_Providers_Representation_Records_of_Decedent.pdf</a></td>
</tr>
<tr>
<td>Electronic Communications</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12164/policy_12164.pdf?_=0.681979083131">https://hpo.johnshopkins.edu/enterprise/policies/170/12164/policy_12164.pdf?_=0.681979083131</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_forms)/A_5_3_b_Providers_Request_Electronic_Communications_JH_Provider_Patient.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_forms)/A_5_3_b_Providers_Request_Electronic_Communications_JH_Provider_Patient.pdf</a></td>
</tr>
<tr>
<td>Faxing PHI</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12163/policy_12163.pdf?_=0.00281418964642">https://hpo.johnshopkins.edu/enterprise/policies/170/12163/policy_12163.pdf?_=0.00281418964642</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_plans_forms)/AB_5_2_a_Providers_Plans_Fax_Transmittal_Cover_Sheet.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/docs/policies_and_forms(provider_plans_forms)/AB_5_2_a_Providers_Plans_Fax_Transmittal_Cover_Sheet.pdf</a></td>
</tr>
<tr>
<td>Health Oversight Activities</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12184/policy_12184.pdf?_=0.507401411088">https://hpo.johnshopkins.edu/enterprise/policies/170/12184/policy_12184.pdf?_=0.507401411088</a></td>
<td>N/A</td>
</tr>
<tr>
<td>HIPAA Workforce Training</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12207/policy_12207.pdf?_=0.561327616538">https://hpo.johnshopkins.edu/enterprise/policies/170/12207/policy_12207.pdf?_=0.561327616538</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Involvement of Another in an Individual's Care</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12176/policy_12176.pdf?_=0.00603413770951">https://hpo.johnshopkins.edu/enterprise/policies/170/12176/policy_12176.pdf?_=0.00603413770951</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Topics</td>
<td>Quick Link to Policy</td>
<td>Quick Link to Related Form (if applicable)</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Judicial and Administrative Proceedings</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12202/policy_12202.pdf?_=0.872167011418">https://hpo.johnshopkins.edu/enterprise/policies/170/12202/policy_12202.pdf?_=0.872167011418</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12198/policy_12198.pdf?_=0.0294755325474">https://hpo.johnshopkins.edu/enterprise/policies/170/12198/policy_12198.pdf?_=0.0294755325474</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Minimum Necessary</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12206/policy_12206.pdf?_=0.735246916663">https://hpo.johnshopkins.edu/enterprise/policies/170/12206/policy_12206.pdf?_=0.735246916663</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12137/policy_12137.pdf?_=0.205934961466">https://hpo.johnshopkins.edu/enterprise/policies/170/12137/policy_12137.pdf?_=0.205934961466</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_a_Providers_NPP.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_a_Providers_NPP.pdf</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_b_Providers_Acknowledgment_Receipt_NPP.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_b_Providers_Acknowledgment_Receipt_NPP.pdf</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_c_Providers_Refusal_Sign_Acknowledgment_Receipt_NPP.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_1_1_c_Providers_Refusal_Sign_Acknowledgment_Receipt_NPP.pdf</a></td>
</tr>
<tr>
<td>Portable Electronic Devices</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12215/policy_12215.pdf?_=0.707059273706">https://hpo.johnshopkins.edu/enterprise/policies/170/12215/policy_12215.pdf?_=0.707059273706</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Privacy Complaints</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12219/policy_12219.pdf?_=0.0142146611322">https://hpo.johnshopkins.edu/enterprise/policies/170/12219/policy_12219.pdf?_=0.0142146611322</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_plans_forms/AB_11_1_a_Providers_Plans_Privacy_Complaint_Information_Sheet.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_plans_forms/AB_11_1_a_Providers_Plans_Privacy_Complaint_Information_Sheet.pdf</a></td>
</tr>
<tr>
<td>Public Health</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12185/policy_12185.pdf?_=0.242096878293">https://hpo.johnshopkins.edu/enterprise/policies/170/12185/policy_12185.pdf?_=0.242096878293</a></td>
<td>N/A</td>
</tr>
<tr>
<td>Request to Amend Health Records</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12170/policy_12170.pdf?_=0.7776627248">https://hpo.johnshopkins.edu/enterprise/policies/170/12170/policy_12170.pdf?_=0.7776627248</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_6_3_a_Providers_Request_Amend_PHI.pdf">http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_6_3_a_Providers_Request_Amend_PHI.pdf</a></td>
</tr>
</tbody>
</table>
## Appendix B

<table>
<thead>
<tr>
<th>Topics</th>
<th>Required by Law</th>
<th>Restriction Requests</th>
<th>Right to Access Own Health Record</th>
<th>Social Media</th>
<th>Taking PHI Off-Site</th>
<th>Treatment, Payment and Health Care Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required by Law</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12204/policy_12204.pdf?_=0.0210638510178">https://hpo.johnshopkins.edu/enterprise/policies/170/12204/policy_12204.pdf?_=0.0210638510178</a></td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12168/policy_12168.pdf?_=0.600869528312">https://hpo.johnshopkins.edu/enterprise/policies/170/12168/policy_12168.pdf?_=0.600869528312</a></td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12169/policy_12169.pdf?_=0.750277695646">https://hpo.johnshopkins.edu/enterprise/policies/170/12169/policy_12169.pdf?_=0.750277695646</a></td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12214/policy_12214.pdf?_=0.0372430216043">https://hpo.johnshopkins.edu/enterprise/policies/170/12214/policy_12214.pdf?_=0.0372430216043</a></td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12216/policy_12216.pdf?_=0.327245152496">https://hpo.johnshopkins.edu/enterprise/policies/170/12216/policy_12216.pdf?_=0.327245152496</a></td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12205/policy_12205.pdf?_=0.0861176825688">https://hpo.johnshopkins.edu/enterprise/policies/170/12205/policy_12205.pdf?_=0.0861176825688</a></td>
</tr>
<tr>
<td>Restriction Requests</td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/">http://intranet.insidehopkinsmedicine.org/privacy_office/</a> docs/policies_and_forms/provider_forms/A_6_1_a_Providers_Contract_HITECH_Insurance_Restriction_Healthcare_Services.pdf?_=<a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12168/policy_12168.pdf?_=0.600869528312">https://hpo.johnshopkins.edu/enterprise/policies/170/12168/policy_12168.pdf?_=0.600869528312</a></td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/">http://intranet.insidehopkinsmedicine.org/privacy_office/</a> docs/policies_and_forms/provider_forms/A_6_1_b_Providers_Request_Patient_Restriction_Self_Pay.pdf</td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/">http://intranet.insidehopkinsmedicine.org/privacy_office/</a> docs/policies_and_forms/provider_forms/A_6_1_c_Providers_Handout_Patient_Counseling.pdf</td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/">http://intranet.insidehopkinsmedicine.org/privacy_office/</a> docs/policies_and_forms/provider_forms/A_6_1_d_Providers_Plan_Request_Restriction_Release_Health_Information.pdf</td>
<td><a href="http://intranet.insidehopkinsmedicine.org/privacy_office/">http://intranet.insidehopkinsmedicine.org/privacy_office/</a> docs/policies_and_forms/provider_forms/AB_6_1_d_Providers_Plan_Request_Restriction_Release_Health_Information.pdf</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to Access Own Health Record</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12169/policy_12169.pdf?_=0.750277695646">https://hpo.johnshopkins.edu/enterprise/policies/170/12169/policy_12169.pdf?_=0.750277695646</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Social Media</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12214/policy_12214.pdf?_=0.0372430216043">https://hpo.johnshopkins.edu/enterprise/policies/170/12214/policy_12214.pdf?_=0.0372430216043</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Taking PHI Off-Site</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12216/policy_12216.pdf?_=0.327245152496">https://hpo.johnshopkins.edu/enterprise/policies/170/12216/policy_12216.pdf?_=0.327245152496</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Treatment, Payment and Health Care Operations</td>
<td><a href="https://hpo.johnshopkins.edu/enterprise/policies/170/12205/policy_12205.pdf?_=0.0861176825688">https://hpo.johnshopkins.edu/enterprise/policies/170/12205/policy_12205.pdf?_=0.0861176825688</a></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---
Checklist for Privacy Compliance

The Checklist for Privacy Compliance is provided as a self-assessment tool to allow Johns Hopkins covered entities and functions to gauge, in broad terms, their level of compliance with the Johns Hopkins privacy policies and requirements. While this checklist highlights major aspects of the Johns Hopkins privacy policies and requirements for providers, it should not be viewed as an all-inclusive list. Management is still responsible for compliance with all aspects of the Johns Hopkins policies and program.

It is recommended that you complete this self-assessment at least once every year and keep a file copy of each checklist after it has been completed. Contact the JH Privacy Office for questions regarding the checklist.

View of checklist:

<table>
<thead>
<tr>
<th>Entity: ___________________</th>
<th>Department: ___________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed by: ______________</td>
<td>Date completed: ______________</td>
</tr>
</tbody>
</table>

**JOHNS HOPKINS HIPAA POLICY TEMPLATES**

1. Has the legal entity of which the department is a part (e.g. JHH, BMC, HCGH), or the department itself, formally adopted the JH HIPAA privacy and security policy templates and forms? [http://www.insidehopkinsmedicine.org/hipaa]

2. Has department administration developed departmental policies and procedures to implement the JH HIPAA privacy and security policy templates and forms?

3. Are these departmental policies and procedures available in a written format and easily accessible to workforce members?

4. Do workforce members understand these departmental policies and procedures and how they relate to maintaining the privacy and security of patient information?

**GENERAL PRIVACY AWARENESS**

5. Is there a general culture of respect for the privacy of the patient and his/her protected health information?

6. Do workforce members understand and respect the need to maintain confidentiality?

7. Are workforce members aware of and understand the minimum necessary requirement with respect to use and disclosure of PHI?

8. Do workforce members have a general understanding of what it means for a

To access the full Checklist for Privacy Compliance, visit: [http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/policies_and_forms/provider_forms/A_4_4_1_Providers_Checklist_Privacy_Compliance.pdf].