ADMINISTRATIVE POLICY MANUAL	THE CHILDREN'S HOSPITAL OF PHILADELPHIA Title: CONFIDENTIALITY OF PATIENT AND INSTITUTIONAL INFORMATION	No. A-3-05 Page 1 of 10 Effective Date: 05/23/2022

TABLE OF CONTENTS

POLICY

The Hospital has guidelines to safeguard Patient and Institutional Information from unauthorized access, Use and Disclosure in accordance with applicable law.

SCOPE

This policy applies enterprise-wide to Trustees, Officers, employees and members of the Medical Staff of The Children's Hospital of Philadelphia, the CHOPPA Practice Plans (currently Children's Anesthesiology Associates, Children's Health Care Associates, Children's Surgical Associates, Radiology Associates of Children's Hospital, and their New Jersey Affiliates) (together, the Hospital), and entities controlling, controlled by or under common control with the Hospital, as well as others providing health care services at facilities owned or operated by the Hospital and other persons whose presence at or affiliation with the Hospital may place them in a position to have direct or indirect access to Patient or Institutional Information.

RELATED DOCUMENTS

Administrative Policy Manual	A-1-04	Organizational Ethics Statement
Administrative Policy Manual	A-1-05	Compliance Standards of Conduct
Administrative Policy Manual	A-2-01	Expenditure and Signature Authority

Administrative Policy Manual	A-3-4	Patent and Intellectual Properly Policy
	A-3-12	Information Security Policy
Administrative Policy Manual		
Administrative Policy Manual	A-3-14	Privacy of Patient Information
	Job Aid	Guidelines to Determine Corrective/Disciplinary Action Related to Violations of Hospital Privacy / Information Security Policies
	Job Aid	Incidental Disclosures of Patient Information
	Job Aid	Guidelines for Determining When Access to the Patient Health Record is Job-Related
Administrative Policy Manual	A-4-25	Securing Paper Patient Health Record and Documents Containing Patient Information
Patient Care Manual	IC-2-01	HIV (Human Immunodeficiency Virus)
Patient Care Manual	IM-2-03	Verifying Identity and Authority of Requestors for Release of Information
Patient Care Manual	IM-2-04	Storage and Release of Mental Health Records and HIPAA Psychotherapy Notes, Pennsylvania
Patient Care Manual	NJ-IM-1-03	Storage and Release of Mental Health Records and HIPAA Psychotherapy Notes, New Jersey
Patient Care Manual	IM-3-01	Addendum / Correction to Patient Health Record
Patient Care Manual	RI-2-03	Recording of Patients
Patient Care Manual	RI-5-01	Consent for Care: Pennsylvania Consent for Care: New Jersey
Human Resources Manual	5-2	Rules of Conduct
Human Resources Manual	5-11	Employee Records
Research Policy Manual		Use and Disclosure of Protected Health Information for Research

I. DEFINITIONS

A. Business Associate: A person (who is not part of the Hospital Workforce) or entity that creates, receives, maintains or transmits Patient Information on behalf of the Hospital. A Business Associate may provide, for example, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

B. Disclosure: The release, transfer, provision of access to, or divulging in any other manner of

information outside the Hospital or to an individual who is not part of the Hospital's Workforce.

C. Institutional Information: Any information whether oral, electronic, or on paper that involves Workforce Member Data, non-public Hospital business information, Non-public Research Information, vendor trade secrets, or other confidential Hospital information.

D. Minimum Necessary: The least information necessary to accomplish the intended purpose of the Use, Disclosure or request.

E. Non-public Research Information – Information generated through or as part of research activities including, but not limited to, Hospital data that has been converted into research data, in either identifiable or de-identified form, which has not been published or otherwise made public in accordance with this policy.

F. Patient: The Hospital patient, current or former, whether inpatient or outpatient, who is the subject of the information.

G. Patient Information: Information, whether oral, electronic, or on paper, that (1) may identify a Patient or his/her relatives, employers, or household members; and (2) is created or received by the Hospital and relates to an individual's past, present or future physical/mental health or condition, the provision of health care or the past, present, or future payment for health care. This includes the following identifiers: names; addresses; telephone numbers; all dates directly related to a Patient, including any of the following: birth date, admission dates, discharge dates, date of death; fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying numbers, characteristics, or codes that may identify individual Patients, including their initials.

H. Personal Representative: A person who, under state law, has the authority to act on behalf of a Patient in making decisions related to health care. The parent/legal guardian of a minor is generally treated as a minor's Personal Representative as is any person designated by court order

as the minor's legal guardian or as a person who can otherwise make medical decisions on behalf of a minor. For deceased Patients, an executor, administrator or other person who has the authority to act on behalf of such deceased Patient's estate is treated as the Personal Representative of the deceased with respect to information relevant to such personal representation. The following situations are exceptions:

1. For health care services for which the minor consents for him/herself under applicable law and the Hospital's Policy: Consent for Care in Pennsylvania and Policy: Consent for Care in New Jersey (e.g., if the minor is emancipated or the minor can consent to the type of services at issue, such as for treatment of sexually transmitted diseases) and the minor has not requested that his/her parent or guardian be treated as a Personal Representative;
2. For health care services as to which the minor's parent/guardian accepts an agreement of confidentiality between the minor and his/her care providers; and
3. If the Hospital has a reasonable belief that the Patient has been or may be subjected to domestic violence, abuse or neglect by such person or that treating such person as the Patient's Personal Representative could endanger the Patient, and the Patient's Attending Physician or his/her designee determines that it is not in the best interest of the Patient to treat the person as the Personal Representative of the Patient.

I. **Safeguards: Administrative, technical and physical** precautions utilized by Hospital Workforce members to protect against any reasonably anticipated threat to the privacy of Patient Information such as unauthorized Use and/or Disclosure of the information. Reasonable Safeguards are to be utilized to protect Patient Information in all forms, including oral, written and electronic.

J. **Use:** The sharing, employment, application, utilization, examination, or analysis of Patient Information and Institutional Information within the Hospital or by an individual who is part of the Hospital's Workforce.

K. **Vendor:** Entities and persons that have or are seeking to enter into business relationships with the Hospital (e.g., to provide any equipment, product, supply, facility, item or service for which payment may be made, including but not limited to a pharmaceutical product, medical device, or other clinical equipment, product or supply), as well as the representatives and agents of such entities or persons.

L. **Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance

of work for the Hospital, is under the direct control of the Hospital, whether or not they are paid by the Hospital.

M. Workforce Member Data: Any of the following information about the Hospital's Workforce maintained by the Hospital that is not lawfully available to the general public from Federal, State or local government records:

1. Personally Identifiable Information (PII) that includes first name or first initial and last name of Workforce member in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

- Social Security number.
- Driver's license number or a State identification card number issued in lieu of a driver's license.
- Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

2. Other information associated with a particular Workforce member such as:

a. Personal contact information
b. Compensation or Benefits related
c. Performance or talent management related
d. Payroll related
e. Personal demographics (Sex, Gender Identity, Race/Ethnicity, Disability, Age, Veteran Status)
f. Emergency contact or family information
g. Employee Health Information that the Hospital creates, receives or maintains about a Workforce member's health in the Hospital's capacity as an employer (e.g., information a Workforce member might provide when seeking a workplace accommodation for a disability and information the Hospital collects to determine fitness for duty). Such Employee Health Information is an employment record.
h. Other personal information maintained by the Hospital

II. GENERAL GUIDELINES RELATED TO PATIENT AND INSTITUTIONAL INFORMATION

A. Permitted Use and Disclosure. Patient and Institutional Information is only permitted to be accessed, Used or Disclosed by persons within the scope of this Policy to the extent necessary for job performance in accordance with Hospital policies. Any access, Use or Disclosure of Patient or Institutional Information for any other purpose is a violation of this Policy and can result in disciplinary action up to, and including, termination and legal action.

B. Ownership of Patient and Institutional Information. All such information is the property of the Hospital. At the conclusion of a Workforce member's affiliation with the Hospital, any such information in the individual's possession must be returned to the Hospital unless otherwise agreed to in writing by the Hospital.

C. Safeguarding Information. Persons within the scope of this Policy must use reasonable Safeguards to maintain the confidentiality of Patient and Institutional Information. Workforce members are responsible for using reasonable Safeguards when accessing, handling, communicating, transmitting, transporting and discarding Patient and Institutional Information to prevent unauthorized Use or Disclosure. Examples of such Safeguards include, but are not limited to:

i. Using and Disclosing the Minimum Necessary information needed for a task or communication when the purpose is not related to a patient's care.

ii. Utilizing safety behaviors for error prevention such as paying attention to detail using the self-checking method of STAR (Stop, Think, Act, Review) when Disclosing information to avoid unintentional, unauthorized Disclosure.

iii. Physically securing Hospital-issued electronic devices that contain Patient or Institutional Information to prevent loss or theft of the devices and/or data contained on them.

D. Reporting incidents involving unauthorized access, Use, Disclosure, loss or theft of Patient or Institutional information or devices containing such information. Any incident involving unauthorized acquisition, access, Use or Disclosure of Patient or Institutional Information or devices containing such information must be reported immediately for investigation. Any incident involving electronic data or loss/theft of an electronic device is to be reported to IS Help Desk at 4-HELP. All other incidents are to be reported to the Hospital's Safe to Say compliance reporting line at 1-866-246-7456 or to the Office of Compliance and Privacy at (267) 426-6044 or PrivacyOffice@chop.edu.

i. Protection from Retaliation. The Hospital will not take any action against a Workforce member for reporting an incident in good faith. If a Workforce member is a party to a reported incident, the Workforce member's good faith efforts will be considered in assessing whether disciplinary action against the Workforce member is appropriate

E. Role of Privacy Officer and Chief Information Security Officer. The Hospital's Patient Privacy program is overseen by the Privacy Officer who is the Chief Compliance Officer. The Hospital's Security program is overseen by the Chief Information Security Officer. The role of these officers is outlined in supporting Hospital policies referenced above.

F. Mitigation and Breach Notification. The Hospital takes action to the extent practical to reduce known harmful effects of an unauthorized Use or Disclosure of Patient Information and PII. The Office of Compliance and Privacy in consultation with the Office of General Counsel determines whether an incident constitutes a breach or otherwise requires notification to affected individuals under federal or state law and coordinates such notification.

G. Vendors and Patient Information. The Hospital enters into a written Business Associate Agreement (BAA) with Business Associates. All proposed arrangements with individuals and/or organizations that involve Use or Disclosure of Patient Information, including renewals or amendments of existing agreements, are to be reviewed to determine if a BAA is needed. For agreements involving purchased products and/or services, the Hospital's Supply Chain department is responsible for ensuring that a written BAA is entered into when needed for all such agreements. For agreements that are outside the purview of Supply Chain, it is the responsibility of the person authorized under the Hospital's Expenditure and Signature Authority policy or the Research Institute's Signature Authority Matrix to review such agreements to ensure that a written BAA is entered into when required by law. A copy of any executed BAA must be provided to Supply Chain to maintain copies of BAAs for the Hospital.

H. Vendors and Institutional Information. For agreements involving purchased products and/or services (including services provided in support of a research project) the Hospital's Supply Chain department must be consulted to ensure that all appropriate confidentiality provisions are entered into when needed for all such agreements. For agreements that are outside the purview of Supply Chain, it is the responsibility of the person authorized under the Hospital's Expenditure and Signature Authority policy or the Research Institute's Signature Authority Matrix to review such agreements to ensure appropriate confidentiality provisions are included.

I. Media Requests for Patient and Institutional Information. Requests by representatives of the news media should be referred to the Public Relations Department during business hours or the on-call Public Relations representative during evenings, nights and weekends.

III. Patient Information.

A. Relationship to Other Policies and Materials. This Policy states general standards for access, Use and Disclosure of Patient Information and incorporates by reference the Hospital's detailed policies implementing the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 and its regulations (HIPAA) and the Hospital's Notice of Privacy Practices.

B. Permitted Use and Disclosure of Patient Information. Patient Information may only be Used and/or Disclosed in accordance with Hospital policies, the Hospital's Notice of Privacy Practices or in other situations when allowed or required to do so by law.

C. Specially Protected Patient Information. Certain types of Patient Information is afforded additional protection under federal and/or state law as it applies to Disclosure of or access to such information. See related Hospital policies for details. Examples of such include:

i. HIPAA Psychotherapy Notes written and maintained by a mental health professional;
ii. Mental health records documented by a mental health provider;
iii. HIV-related information;
iv. Substance (drug and alcohol) diagnosis or treatment information;
v. Genetic information Disclosed to certain non-healthcare providers.

D. Medical Records, Billing Records and Other Patient Related Information. All paper and electronic medical records, billing records and information about Hospital Patients, including Patient lists, photographs of Patients and all other documentation and files containing Patient Information are confidential and the property of the Hospital.

E. Non-Confidential Directory Information about Inpatients. In response to an inquiry about a specifically named Patient who is an inpatient, persons within the scope of this Policy may verify that an individual is an inpatient and provide the Patient's room and telephone number and general condition (e.g., undetermined, good, fair, serious, critical), if available, unless the Patient/Personal Representative has objected to Disclosure of directory information during the Hospital stay.

F. Recording or Photographing Patients. Requests to record or photograph a Patient (including still, videotape, audiotape and/or film) are governed by Hospital policy: Recording of Patients.

G. Employee Health Information that is PHI. Individually identifiable health information about Workforce members created, received or maintained in the Hospital's capacity as a health care provider or by the Hospital's employer sponsored group health plan is Patient Information and is subject to applicable Hospital policies related to the Privacy of Patient Information and Security of confidential information.

IV. Institutional Information.

A. Workforce Member Data.

1. **Requests for data that is Personally Identifiable Information (PII).** Unless authorized in writing by the Workforce member to whom the PII belongs, Disclosure and Use of Workforce PII is permitted only on a Minimum Necessary basis and in accordance with Hospital Policies, written Hospital guidance and legal requirements.
2. **Requests for Other Workforce Member Data.** The Hospital allows leaders to access, Use and Disclose such data in the Workday system as needed to perform their job. Access to Workforce Member Data outside of what is available to a leader in the Workday system is evaluated by the Human Resources department on a case-by-case basis to validate business justification and Minimum Necessary.
3. **Maintenance of Workforce Member Data.**
   i. Employee Health Information must be maintained separate from the employee's personnel files in accordance with applicable employment laws.
   ii. All other Workforce Member data, including PII, is maintained in accordance with applicable law.

B. Non-public Research Information. All Non-public Research Information is to be kept confidential unless the release of such information is consistent with academic standards and any contractual obligations. Non-public Research Information should not be provided outside of the Hospital unless it is being provided for (i) academic publication or scientific meeting in accordance with academic practice or (ii) another academic purpose and pursuant to an agreement executed by an authorized administrative unit (e.g., CHOP's Office of Sponsored Projects, Office of Collaborative and Corporate Research Contracts, etc.). The provision of Non-public Research Information to vendors is addressed in section II.H above.

1. Requests for Non-public Research Information for purposes other than academic activities, presentations and publications should be directed to the Chief Scientific Officer (CSO), or their designee. Other executive-level decision makers may also be involved depending on the nature of the information sharing and the third party with whom it is being shared. Questions about whether data is Non-public Research Information can be directed to the CHOP CSO or designee.

C. Trade Secrets. This includes Hospital and vendor trade secrets (e.g., computer software), and other vendor confidential information. Such information is to be kept confidential unless the release of such information is consistent with contractual obligations and specifically authorized by a written Hospital policy and a Hospital Senior Vice President or above. Trade secrets may

not be provided outside of the Hospital unless, at a minimum, a written confidentiality agreement is entered into between CHOP and the third party on a CHOP form approved through the appropriate internal channels.

D. **All Other Institutional Information**. Such information is to be kept confidential and its Disclosure is permitted only on a Minimum Necessary basis and with the approval of applicable Hospital Senior Vice President or at their designee.

V. Sanctions. Any member of the Hospital Workforce who violates any provision of this policy or of applicable laws or regulations may face sanctions up to and including discharge and/or removal from the medical and research staffs, as appropriate, depending on the seriousness of the violation. In addition, some activities may lead to risk of civil and criminal liability.

RESPONSIBILITY FOR MAINTENANCE OF THIS POLICY

GENERAL COUNSEL
CHIEF COMPLIANCE OFFICER

Supersedes	Approved by:
05/17/2021	_____ **Douglas G. Hock, EVP & System Chief Operating Officer**