Policy Name: Use of Patient Information by the Hospital and Medical Staff

Applies to: OSU Wexner Medical Center [University Hospital, East Hospital, Brain and Spine Hospital, Richard M. Ross Heart Hospital, Harding Hospital, Dodd Rehabilitation Hospital, Ambulatory Clinics and Services] and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute and Outreach Sites

Policy Objective

The Ohio State University Wexner Medical Center (OSUWMC) and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute (The James) is committed to keeping patient information safe and secure. As demonstration of the commitment to patient privacy and protection of PHI, the HIPAA compliance program is constructed of various Standard Operating Procedures, general practices, and the following policy.

Definitions

Term	Definition
Access	The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.
Authorization	Written permission from a patient or patient's Personal Representative for Use and/or Disclosure of PHI that meets the requirements of the HIPAA Privacy Rule.
Disclosure	Releasing, transferring, giving access to or divulging PHI outside of the Medical Center.
Health Care Operations	Medical Center activities that are related to covered functions including but not limited to: 1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about Treatment alternatives; and related functions that do not include Treatment; 2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; 3. Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care; 4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; 5. Business planning and development, such as conducting cost- management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of Payment or coverage policies; and 6. Business management and general administrative activities of the Medical Center, including, but not limited to: i. Management activities relating to implementation of and compliance with the requirements of the Privacy Rule and HIPAA; ii. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer. iii. Resolution of internal grievances; iv. The sale, transfer, merger, or consolidation of all or part of the Medical Center with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and v. Creating de-identified health information or a limited data set, and fundraising for the benefit of the Medical Center.

Policy Name: Use of Patient Information by the Hospital and Medical Staff

Applies to: OSU Wexner Medical Center [University Hospital, East Hospital, Brain and Spine Hospital, Richard M. Ross Heart Hospital, Harding Hospital, Dodd Rehabilitation Hospital, Ambulatory Clinics and Services] and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute and Outreach Sites

Health Insurance Portability and Accountability Act (HIPAA)	Federal regulations that establishes the minimum level of protection for patient information and the administrative steps for compliance.
Medical Center	OSU Wexner Medical Center [University Hospital, East Hospital, Brain and Spine Hospital, Richard M. Ross Heart Hospital, Harding Hospital, Dodd Rehabilitation Hospital, Ambulatory Clinics and Services] and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute and Outreach Sites and College of Medicine
Payment	Activities undertaken by a health care provider or health plan related to obtaining or providing reimbursement for the provision of health care or the activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan.
Protected Health Information (PHI)	Individually identifiable information (oral, written or electronic) about a patient's past, present, or future physical or mental health, the receipt of health care, or Payment for that care. This includes the PHI of deceased individuals, unless the individual has been deceased for more than 50 years.

Policy Details

A. Patient Information Use and Security
Hospital staff, students, researchers and volunteers who have been properly trained in patient confidentiality are authorized to use Patient Information for the following purposes:
1. Treatment: Patient Information is to be accessed and shared only by those members of the Hospitals' and medical staff actively involved in the treatment of the patient, including the referring physician and any consulting physician on staff.
2. Payment: Designated departments are permitted to access Patient Information necessary to obtain reimbursement for patient care services and reimbursable research expenses.
3. Operational, Educational or Business Purposes: Authorized members of the medical staff or Hospitals staff are permitted access and Use Patient Information for appropriate operational, educational or business purposes of the Hospitals.
4.

B. Security, Confidentiality and Ownership
All Patient Information maintained by OSUWMC/The James (herein referred to as the Hospitals) is confidential.
1. The physical form of Patient Information (including files, data bases, microform, printouts, etc.) is the property of the Hospitals.
2. The Hospitals will regulate the storage, access, release, transmission, and disposal of all Patient Information and other sensitive data for both internal and external use, and has established the minimum security standards for Patient Information described in this Policy. Please refer to Patient Information and HIPAA Requirements 09-03.

Procedure

A. Use for Treatment, Payment, Educational and Business Access Purposes
1. Access to Patient Information
    a. Access to Hospital Patient Information will be provided to Hospital users (as defined below) who have completed all required training.
    b. All requests for access to patient information and medical records are subject to review by Medical Information Management staff, Information Security, and Hospitals Administration.
    c. Access will be denied/de-activated if such privilege would not be in the best interest of the patient or the Hospitals, or such access has been abused.
2. Format of Patient Information
    a. Electronic Information: Access to electronic information must be approved and for appropriate

purposes, and must comply with all applicable hospital and departmental policies and procedures.

b. For clinical applications managed by Information Systems:
   i. Users must complete an eServices request to gain access to clinical applications.
   ii. Users requiring remote access must complete a Remote Access Request Form

3. Medical Information Management (MIM) is the custodian of the record.
   a. Paper records may be accessed for treatment, payment or operations.
   b. Access to and sign out of hard copy medical records is granted according to MIM Standard Operating Procedure. Please see MIM website
   c. Medical records must be kept secure and returned promptly when no longer needed.
4. Copying of Patient Information
   a. Only authorized staff may copy Patient Information.
   b. Copying of Patient Information will be performed according to Medical Information Management Standard Operating Procedure and Guidelines.
   c. Oral information: Patient Information in oral format must be kept private and secure in accordance with the OSUWMC/The James Confidentiality Policy.
5. Users
   a. Medical Staff with clinical access privileges: All medical staff with privileges at OSUWMC/The James will be granted access to electronic medical records, upon request (e.g., IHIS).
   b. Nursing, ancillary, and clerical staff: All nursing, ancillary and clerical staff affiliated with OSUWMC/The James through direct employment with the Medical Center and a documented need to know shall be granted access to the EMR. If the nursing, ancillary and clerical staff member is not employed by the Hospitals, access to the electronic medical record may be granted, upon request, via onboarding or account modification request submitted by the sponsor.
   c. Temporary Staff, Consultants, Vendors and Physician Billing Offices
      i. Each agency and billing office will be required to complete a Vendor Agreement and each employee must sign a Confidentiality Statement.
      ii. Temporary staff of the Medical Center in a role with a documented need-to-know may be granted access to electronic medical records (e.g., IHIS with an expiration period of twelve months).
      iii. If additional access is required, the appropriate supervisor must request an extension through account modification request.
      iv. Staff from credit and collection agencies will be allowed to have access in order to assist with the billing process.
   d. Students
      i. All medical, nursing and pharmacy students will be given access to the electronic medical record upon request, where appropriate.
      ii. This access will be established with an expiration period of one year. If after two years the individual does not access the system, the account will be deleted.

B. Use of Patient Information in Case Reports
1. Faculty and trainees publishing case reports in publications and/or peer reviewed journals that involve a wide distribution must: (1) de-identify the case study; (2) obtain signed patient authorization or if the patient is deceased, signed authorization from the executor of the patient's estate, and if no executor, signed authorization from the patient's next of kin; or (3) receive special permission from the Chief Clinical Officer/Chief Medical Officer for the OSUWMC/The James or designee to publish the case report without signed patient authorization.
2. Case Presentations to Peers: Faculty and trainees presenting case reports at conferences to clinician peers may use de-identified radiology and pathology images along with limited de-identified clinical history without patient authorization. While this de-identified information is presented to clinician colleagues at conference sessions, the

information is not widely distributed such as case reports published in peer reviewed-journals. However, where the case presented is extremely rare and the de-identified information could be used to recognize the patient, faculty and trainees must obtain the patient's authorization. See Privacy Website and Release of Patient Information for Media, Educational Purposes, or Case Studies Form

C. Use of Quality Data
   1. If the project will use quality data, approval must be sought from the Medical Director through the Department of Quality and Operations Improvement.

D. Use for Clinical Evaluation
   1. If the project involves the evaluation of another OSU clinician's practice or outcomes and the clinician is not a co-investigator on the study, the investigator must obtain the consent of the physician and/or the physician's chair before initiating the study.

E. Use of Patient Information for Other Purposes
   1. Workforce members must not place PHI on social media without obtaining the appropriate patient authorizations and Medical Center approval. Please refer to Social Media 05-05 and Patient Information and HIPAA 09-03 for more information on the use of social media.

F. Required Security Procedures
   1. Compliance with the HIPAA Security Rule relies on the Information Security Policy 07-06. Where a standard exists that supports policy details, compliance with the policy will be measured by compliance with the standard. Unless otherwise noted in the Information Security Policy, the Medical Center is to follow OSU Information Security Control Requirements as defined in the Information Risk Management Framework (cybersecurity.osu.edu/iscr).

G. Use of Portable Storage for Patient Information
   1. Sensitive Patient Information must be encrypted in accordance with the Information Security Policy 07-06.
   2. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

H. Access to Information Systems Holding Patient Information
   1. User access to systems is addressed in the Information Security Policy 07-06.
   2. Access is limited to situations in which a legitimate business need and purpose can be demonstrated.
   3. HIPAA requires logging and monitoring of all access to patient information.
      a. Users should only access information required to perform their job duties.
      b. Users are responsible for accesses made under their user ID and password.
      c. Information systems will be monitored to detect unauthorized conduct.

I. Release of Patient Information by Information Systems to Third Parties Outside the Hospital
   1. Only staff authorized to release confidential information may do so. Those authorized to release confidential information include Medical Information Management and others authorized by Medical Information Management.
   2. Medical Information Management is responsible for managing the release of patient information pursuant to a valid patient authorization. Please see Release of Information to Patients 09-09
   3. Sensitive Patient Information that is transmitted outside the Medical Center network (e.g. email, FTP, etc.) must be encrypted. See Information Security Policy 07-06.

Policy Name: Use of Patient Information by the Hospital and Medical Staff

Applies to: OSU Wexner Medical Center [University Hospital, East Hospital, Brain and Spine Hospital, Richard M. Ross Heart Hospital, Harding Hospital, Dodd Rehabilitation Hospital, Ambulatory Clinics and Services] and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute and Outreach Sites

J. Disposal of Patient Information by Information Systems
   1. Devices that store Patient Information must be disposed of in a manner that meets the minimum requirements in the Risk Management Framework.

K. Failure to Adhere to this Policy
   1. Failure to adhere to this policy and procedure may result in corrective action, up to and including termination.

Resources

Pastoral Care 03-03
Management of Inpatient-Outpatient Correctional Institution Inmates and Other Custodial Arrangements 03-09 Management of Inpatient-Outpatient Correctional Institution Inmates and Other Custodial Arrangements 03-09
Social Media 05-05
Communications with the Media & Publicity 05-06
Patient Information and HIPAA 09-03
Release of Information to Patients 09-09
Vendor Access & Control - 09-14
Publicity and Publications 05-07 JAMES
OSUWMC Information Security Policies

Contacts

Office	Telephone
Compliance	614-293-7802
Legal	614-293-8446
Medical Information Management	614-293-8356

History

The Ohio State University Wexner Medical Center		
Approved By (List All Committees): 1. Compliance Committee	*Approval Date:* 1. 12/10/2020	*Issue Date:* 4/1/2003 *Effective Date:* 6/2/2021
Review Cycle: ☐ 2 years ☒ 3 years	*Prior Approval Date(s)*: 04/01/2003	

Arthur G. James Cancer Hospital and Richard J. Solove Research Institute		
Approved By (List All Committees): 1. Compliance Committee	*Approval Date:* 1. 12/10/2020	*Issue Date:* 4/1/2003 *Effective Date:* 6/2/2021
Review Cycle: ☐ 2 years ☒ 3 years	*Prior Approval Date(s)*: 04/01/2003	