THE OHIO STATE UNIVERSITY
WEXNER MEDICAL CENTER

Policy Name: Photography of Patients
Policy Number: 03-37
Organization Name: Health System
Last Revised: June 2015

Applies to: Workforce Members

POLICY

The purpose of this policy is to establish guidelines for the use of cameras and video recording devices within the Ohio State University Health System (OSUHS), and to protect the privacy and security of patients and their confidential information. This policy applies to all workforce members, which include employees, faculty, staff, students and volunteers.

Definitions

Term	Definition
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.
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.
Protected Health Information Image ("PHI-I")	Any identifiable image of a patient or procedure. These images may be stored and transmitted in various manners (see below). Items that could be used to individually identify patients include, but are not limited to: a. The patient's name; b. The patient's Medical Record Number or Encounter Number; c. The patient's face or any part of the face; d. The patient's birth date, admission date, discharge date, date of death; e. The patient's Social security number; f. Any other unique identifying number, characteristic, or code of the patient;

Policy Details

The collection, duplication, disclosing, transmission or storage of Protected Health Information Images (PHI-I), for treatment, payment and operations will be in accordance with the OSU Health System Joint Notice of Privacy Practices.

All PHI-I obtained for clinical purposes are considered to be Protected Health Information and are part of the patient's medical record. Images obtained for non-clinical purposes will require prior Authorization from the patient or their representative. All images shall be maintained in a secure manner to protect patient privacy. No images may be saved on a personal device that is not registered with and properly encrypted by OSUWMC Information Technology.

Only Medical Center approved devices and applications may be used to photograph patients. Please call the Information Technology Help Desk with questions.

Applies to: Workforce Members

I. Patient Photography, Videotaping, and Other Imaging Requiring Authorization

A. Educational and/or Publications and Presentations

1. Photographs or recordings that contain any patient identifiers or facial images are protected PHI-I.
2. Patients may agree to the use and disclosure of their PHI-I for the purpose of publication or presentation by signing the OSUHS Consent and Authorization for Photography form.

B. Documentation of Abuse and Neglect

1. If, after appropriate assessment, it is suspected that the patient is a victim of abuse/neglect, images may be taken after obtaining Authorization from the patient using the OSUHS Consent and Authorization for Photography form.
2. Photographs should be taken of the visible injuries,
3. One set of any images shall be placed in the patient's medical record;
4. Copies of the pictures or images shall be offered to the patient;
5. Please refer to Policy 03-31 Domestic Abuse/Victims of Violent Crime.

C. Law Enforcement

1. When law enforcement agencies request to photograph or videotape a patient, permission may be given if:
    a. The attending physician is of the opinion that the patient's condition will not be jeopardized or compromised by the obtaining of the images;
    b. The attending physician will document the opinion in the patient's medical record; and
    c. The patient or their legal representative authorizes the photography or videotaping by law enforcement.
2. Photographs or images of patients shall not be released to law enforcement without prior patient Authorization.

D. Marketing/Public Relations/Fund Raising/Media

1. The Department of Communications and Marketing shall obtain consent from the patient or their legal representatives.
2. The OSUMC Authorization/Consent for Interview, Photography and/or Video Release of Information form will be used.

E. Research

1. All components of this policy are also applicable to photographs used in research that are uploaded into a medical record. For photographs used in research that will not be uploaded to the Medical Record, your device must be registered per this policy. (See III, A below).
2. Photographs taken as part of a research protocol must be approved by the OSU Institutional Review Board (IRB).
3. Authorization for photography, videotaping, or other imaging must be incorporated into the informed consent document signed by the research subject or the subject's legally authorized representative.

Applies to: Workforce Members

4. If photographs or images of research subjects are disclosed with other researchers, sponsors and/or organizations, those researchers, sponsors and/or organizations must be specifically listed in the "Those Who May Use, Share and Received Your Information As Part of This Study," section of the Ohio State University HIPAA Research Authorization form.

II. Authorization

A. Authorization to Obtain Non-Clinical Images

1. The patient or their legal representative must give written Authorization before photography, videotaping or imaging is obtained using the OSUHS Consent and Authorization for Photography form.
2. If photographs or images are obtained prior to obtaining patient Authorization (e.g. the patient is unconscious), the films, photographs or images shall not be used until appropriate authorization is obtained from the patient or their legal representative.
3. If Authorization cannot be obtained, the films, photographs, videotapes or images should be destroyed by the individual who obtained the image.

B. Disclosure of Images

1. Unless required by law, the disclosure of photographs, videotapes and other images will not be permitted without the Authorization of the patient or their legal representative.
2. The clinician who obtained the images assumes responsibility for the appropriate collection, use, duplication, disclosure, transmission, storage, and deletion of those images.

III. Devices, Storage, Transmission and Retention of Images

A. Devices

1. Prior to utilizing your personal device, you must register your device with OSUWMC Information Technology.
2. To have your device or application approved where it is not already listed on the approved device and application list, contact the Information Technology Help Desk. Staff may direct any questions regarding the approved device processes to the Information Technology Help Desk.

B. Safeguarding of Images

1. All workforce members will be responsible for the protection of PHI-I in their possession, and will safeguard against their improper use and disclosure.
    a. If the PHI-I's are to be part of a patient's medical record, the image taker is responsible for ensuring that the image is properly uploaded and incorporated into the medical record.
    b. If the PHI-I's are not to be part of the patient's medical record (e.g. Images used for educational purposes), they shall be retained at the OSU Medical Center in a secure environment.
        i. Any use shall be consistent with the authorization obtained from the patient;
        ii. Images used outside of the Medical Center, shall be de-identified and maintained in a manner consistent with the provisions of this policy.
2. Security of the data is subject to the provisions of local, state, and federal statutes and regulations, and the provisions of HIPAA privacy policies.

Applies to: Workforce Members

3. It is important that all devices that store electronic PHI-I's have incorporated safeguards to protect data from virus infection and unauthorized access.

C. Storage and Retention of Images

1. Digital image files containing PHI-I's should be stored in a dedicated workspace, not sharing the same space, directory, or memory storage device as personal images.
2. Portable storage media (e.g. compact disks) should be clearly identified with the patient's name, identification number, date and contain the name of the person who is accountable for the images taken.
3. Cameras, CD's, and other storage media containing PHI should be stored securely when not in use.
4. Digital images should be deleted from the storage media (e.g. cameras) when no longer needed.

D. Internet Transmission of Images and Telemedicine

1. Transmission and/or storage of PHI-I across the Internet must be compliant with all HIPAA security standards (i.e. encrypted, password protected) and will require the assistance of the Information Systems Data Security Office.
2. Images created and transmitted during the course of telemedicine treatment should be transmitted in a technically secure environment, along with the medical record.
3. Authorization for use and disclosure of telemedicine images is addressed by a separate policy.

IV. Sanctions

1. Failure to follow this policy will result in sanctions up to and including termination.

Resources

Frequently Asked Questions Regarding Photography in the Clinical Setting

List of Approved Devices and Applications for Photography in the Clinical Setting

Related Policies & Procedures

Patient Information and HIPAA Requirements
Information Security

Contacts

Subject	Office	Telephone
Policy Questions	Security Officer	293-7942
	Privacy Officer	293-4477

History

Issued: January 14, 2008
Revised: June, 2015
Submitted by: HIPAA Steering Committee
Approved by: HIPAA Steering Committee