INDIANA UNIVERSITY

HIPAA-G02
HIPAA Guidance – Safeguarding Patients' Photographs and Recordings

GUIDANCE CONTENT

Effective: August 1, 2013
Last Updated: January 12, 2016

Responsible University Office:
HIPAA Privacy and Security Office

Responsible University Administrator
Vice President for University Clinical Affairs

Guidance Contact:
University HIPAA Privacy Officer
University HIPAA Security Officer

Scope

This guidance applies to all personnel, regardless of affiliation, who have access to Protected Health Information ("PHI") in the form of photography or recordings under the auspices of Indiana University, designated for purposes of complying with the final provisions of the security and privacy rules regulated by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act and laws of the State of Indiana. Please refer to the HIPAA Affected Areas document for a full list of units impacted within Indiana University.

This guidance has been created in conjunction with Indiana University Health and Indiana University Health Physicians and addresses safeguards to apply when accessing, using or disclosing protected health information (PHI) in the format listed above in a manner that is consistent with university policy, IUH policy, IUHP policy, HIPAA or Indiana State Law.

Definitions

See Glossary of HIPAA Related Terms for a complete list of terms.

Reason for Guidance

Photography, audio and/or video recordings of a patient or patient's body part in any medium by IU, IUH or IUHP personnel for the purpose of patient identification, diagnosis, documentation, evaluation, management and/or treatment are a component of the patient's medical record and therefore are to be managed in compliance with medical record description, content and requirements as well as any IU, IUH, and IUHP's confidentiality policies.

As defined in policy, hard copy and digital/electronic photographic images, audio and/or video recordings must be handled in a manner that meets requirements to ensure compliance with IU/IUH/IUHP policy, state and federal law and third party regulatory and accreditation requirements for medical record documentation.

The use of a workforce member's cell phone/smart phone and/or personal camera to photograph or record a patient (and/or any patient body parts) for any workforce member's ***personal, non-business purpose is prohibited***.

Guidance Statement

Exclusions: Unless otherwise specified in this guidance, all photography, audio and/or video recordings and cell phone/smart phone photographs and recordings that are taken in the clinical care setting or in other IUH, IUHP buildings or grounds or IU Clinical or Human Subject Research (including but not limited to clinical trials) areas are covered by this guidance. This guidance document does not apply to the following:

- Victims of suspected child abuse or neglect; refer to the IUH's Child Abuse Manual;
- Photo identification taken at the point of registration; refer to IUH's Patient Access Service policies;
- Marketing and public relations operations as well as for any event that attracts media attention. The IU, IUH or IUHP's Public Relations teams are responsible for coordinating these consents;
- Radiology Images (X-ray, MRI, CT Scan, etc.);
- Ultrasound images;
- De-identified images of internal body part(s) that are taken during a procedure using specialized equipment (e.g., through a lumen). Examples include, but are not limited to Arthroscopy, Endoscopy, Colonoscopy, Colposcopy, -Bronchoscopy, Laparoscopy, etc.;
- EEG Monitoring, EEG Video Monitoring, EEG Intraoperative Monitoring, etc.;
- Pathology slides; and
- Autopsy photographs or recordings taken for purposes of death investigation by a County Medical Examiner's Office
- Video monitoring of premises for security purposes, governed by other policies

I. Equipment/Devices

A. Organizationally Owned and Authorized

Equipment may be used for photography and/or audio and video recording if authorized by Indiana University, Indiana University Health or Indiana University Health Physicians.

Recordings made for IU, IUH, IUHP business purposes or patient care on authorized equipment which may be unsecured (e.g. digital cameras), should be downloaded from the recording device (camera, phone, etc.) to a secure environment, and then immediately deleted from the recording device.

B. Third Party Owned

In general, employee and/or provider personally owned devices are considered third party devices. Third party devices are required to meet IU, IUH, IUHP's security requirements.

The individual is responsible for the security of the device and is required to follow all applicable security policies to implement physical and technical safeguards to protect the device and any data stored on the device.

1. The Device must be encrypted and password protected
2. The Device should be registered with your organization
   a. Indiana University: https://dhcp.iu.edu/
   b. Indiana University Health and Indiana University Health Physicians:
3. Maintain documentation to demonstrate compliance with the requirements document the following information and retain for your records. In the event of a lost or stolen device, this information may be requested by the investigating team.
   a. Take a screen capture of the device showing encryption and a passcode is enabled
   b. Record information about your device and keep for your records including:
      - Model Number
      - Serial Number
      - Mac Address
      - Version of operating system
4. Once the photograph or recording is no longer required on the device and has been properly preserved, the individual is responsible for the proper deletion.

II. Consent Requirements

A. Clinical Purpose: Consent, implied or expressed, to receive care includes consent for the capture of any photograph and/or recording taken or made for clinical purposes.

B. Non-Clinical Purposes:
1. Unless otherwise specified, written consent must be obtained prior to making and/or using a photograph and/or recording for a non-clinical purpose.
2. If a photograph or recording is initially taken, made or used for a Clinical Purpose, and later deemed appropriate for a Non-Clinical Purpose, written consent must be obtained.

Quick Reference Table below

Original Purpose of Photograph or Recording	Consent Form Required	Comment
Clinical Patient Care Purpose and/or Clinical Operations Function	**No**	General consent to treat is obtained
Diagnostic or therapeutic procedures where photography/recording is part of procedure using specialized equipment	**No**	Consent is obtained to undergo the procedure
Future Educational Presentations to teach healthcare clinicians internal or external	**Yes**	
Documentation of trainee's experience	**Yes**	
Quality, safety & performance improvement initiatives	**Yes**	
Celebrations of healing and caring posted in unit or other public space	**Yes**	
Departmental brochures or other publicly displayed media	**Yes**	
Research	**Yes & IRB Approval**	Study Specific Informed Consent & HIPAA Authorization/Approved Waiver
Child Abuse or Neglect and Vulnerable Adult Abuse or Neglect Documentation	**No**	
Domestic Violence	**Yes**	Hospital Personnel
Publicity/Marketing/Media	**Yes**	Obtained by Marketing & Public Relations
By patient/family for personal/private use	**No**	*some restrictions apply

III. Security and Storage

A. Photographs and/or Recordings made and/or used for a clinical patient care purpose must be permanently stored in the patient's medical record in accordance with policy.

B. All other patient photographs and/or video or audio recordings that are not stored in the electronic medical record must be stored in a secure manner that also allows for timely retrieval and protects the patient's privacy. The images must be stored for the retention period required by law, regulation and/or policy and destroyed according to policies governing protected health information.

IV. Deletion of Photographs and Recordings from any Device

Regardless of the ownership of the device, after proper preservation of any patient photograph or recording, the images stored on a digital camera, recording equipment, portable electronic devices memory card and/or any portable device (e.g., flash/thumb drive) must be properly and promptly deleted from the device.

V. *Uses of Photography or Recordings for Educational Purposes*

A. Internal Purposes

Academic, education, training or personnel performance activity provided to or directed only toward IU, IUH or IUHP Audiences and/or IU, IUH, or IUHP patients and their family members. The term includes the use of patient photographs or recordings used for documentation of a trainee's educational experience.

1. Written consent must be obtained and documented in the patient's medical record prior to photographing or recording a patient or a patient's body part for the purpose of Internal Education. Internal Education includes the use of patient photographs or recordings used for documentation of a trainee's educational experience.
2. If patient photography or recording taken or made for a Clinical Purpose is later deemed appropriate for Internal Education, written consent must be obtained prior to the use of the photograph or recording for Internal Education.
3. Patient images produced for the purpose of Internal Education should be de-identified to the extent reasonably possible. If the image cannot be de-identified, all facial identifiers should be removed (e.g., identifiers such as patient name, medical record number and date of birth should be removed or redacted/blocked out, facial images should be cropped so that the entire face is not showing, patient's eyes and nose should be blocked out, etc.)

B. Uses of Photography or Recordings for External Education

Education or training provided to or directed toward non-IU, IUH or IUHP audiences. An example is an educational presentation to members of a state or national specialty or professional organization.

1. Written consent must be obtained and documented in the patient's electronic medical record prior to photographing or recording a patient or a patient's body part for the purpose of External Education. If a patient photography or recording taken or made for a Clinical purpose is later deemed appropriate for External Education, written consent must be obtained prior to the use of the photograph or recording for External Education.
2. Patient images produced for the purpose of External Education must be de-identified (e.g., all identifiers must be removed or redacted/blocked out, including but not limited to patient name, medical record number and date of birth.) If facial images will be used for External Education, they should be cropped so that the entire face is not showing, patient's eyes and nose are blocked out, etc., to the extent reasonably possible for purposes of de-identification of the patient.

VI. Uses of Photography or Recordings for Research

Photographing and/or recording of patient images is allowed if necessary for research purposes, as long as the research has been:

A. Approved by an IU/IUH Institutional Review Board (IRB); and
B. *Appropriate written consent and authorization* of the patient (or the patient's legal representative), as determined by the IRB are obtained; or

C. An IRB approved waiver of informed consent and authorization. Under a waiver, the recordings will need to be de-identified or in the form of a limited data as defined by HIPAA.

VII. REFERENCES

Related Information

A. Indiana University Policies or Guidance

1. HIPAA Privacy & Security Compliance website
   http://protect.iu.edu/compliance/hipaa
2. Uses & Disclosures of Protected Health Information Policy – HIPAA-P01
   https://protect.iu.edu/sites/default/files/HIPAA-P01_-_IU_Uses_and_Disclosures_Policy_Final.pdf
3. Minimum Necessary Policy – HIPAA-P02
   https://protect.iu.edu/sites/default/files/HIPAA-P02_-_Minimum_Necessary_Final.pdf
4. Reporting Security Incidents
   https://protect.iu.edu/cybersecurity/incident
5. Information and Information System Incident Reporting Management and Breach Notification – ISPP-26
   http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-26.shtml
6. Privacy Complaints – ISPP-27
   http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-27.shtml
7. Security of IT Resources – IT-12
   http://policies.iu.edu/policies/categories/information-it/it/IT-12.shtml
8. Mobile Device Security Standard – IT-12.1
   https://protect.iu.edu/cybersecurity/policies/IT12/12.1
9. Best Practices for Handling Electronic Institutional and Personal Information
   http://protect.iu.edu/cybersecurity/data/handling/best-practices
10. Indiana University Standard Operating Procedures for Research Involving Human Subjects
    http://researchadmin.iu.edu/HumanSubjects/hsdocs/IRB_SOPs_5_15_2013.pdf

B. Indiana University Health and Indiana University Health Physicians Policies

1. Photography and Records
   https://pulse.iuhealth.org/depts/PandP/policies/admin/adm2.07.pdf
2. Content of Medical Records
   http://pulse.clarian.org/depts/PandP/policies/admin/adm1-04.pdf
3. Mobile Device Security
   https://pulse.iuhealth.org/depts/PandP/policies/adminis/is1-05.pdf
4. Minimum Necessary
   http://pulse.clarian.org/depts/PandP/policies/hipaa/hipaa3-10.pdf
5. Reasonable Safeguards for Privacy and Confidentiality of Patient Health Information
   http://pulse.clarian.org/depts/PandP/policies/hipaa/hipaa2-01.pdf
6. Uses and Disclosures of Protected Health Information
   http://pulse.clarian.org/depts/PandP/policies/hipaa/hipaa2-11b.pdf
7. Destruction of Protected Health Information and Other Confidential Information
   http://pulse.clarian.org/depts/PandP/policies/hipaa/hipaa4-01.pdf

8. Electronic PHI / Media Disposal and Re-Use
   http://pulse.clarian.org/depts/PandP/policies/adminis/is1-06.pdf
9. Training for Privacy and Security Compliance
   http://pulse.clarian.org/depts/PandP/policies/hipaa/hipaa5-10.pdf
10. Information Security Incident Response
    http://pulse.clarian.org/depts/PandP/policies/adminis/is1-09r.pdf
11. Information Security Incident Response and Security Breach Notification
    http://pulse.clarian.org/depts/PandP/policies/admin/adm1-98.pdf

---

History

05/16/2013	Draft reviewed by IU, IUH, IUHP
07/16/2013	Draft updated by IU, IUH, IUHP
08/08/2013	Final approved by HIPAA Privacy and Security Council
01/12/2016	Updated Definitions Section