The Educational Portfolio and Coaching program requires all students to maintain the professional standards of the College of Medicine in all portfolio entries.\textsuperscript{1,2}

**Use of Patient Images**

Portfolio entries may not include any patient identifying information without the patient’s written consent, in accordance with the requirements of HIPAA\textsuperscript{3} and the policies of the institutions through which the care is provided.\textsuperscript{4,5} Photographs or recordings that contain any patient identifiers or facial images are Protected Health Information Images (PHI-I). Patients may consent to the use and disclosure of their PHI-I for educational purposes by signing the required consent forms supplied by the institutions and practices through which the patients receive care. For OSUMC patients, this would be the OSUHS Consent and Authorization for Photography form\textsuperscript{6} and a Release of Information Form (attached below). Students are required to submit the signed consent forms to the Portfolio Program for secure storage prior to publication of any PHI-I in their portfolios.

Practices and institutions may also have specific policies for patient photography/videography that does not include PHI. Students must refer to and abide by these policies as well. The OSUWMC and Nationwide Children’s Hospital policies for this are included below.

**Use of Images from Global Health Learning Opportunities**

While Global Health Learning Opportunities provide rich learning experiences that can enhance a student’s Showcase Portfolio, use of patient, medical staff or other individual’s images from international clinical experiences is prohibited. Students are encouraged to select artifacts from these experiences that do not include such images. While some images may be permitted in the Global Health Education final report, they may not be used in the Showcase Portfolio.

**Vulnerable Populations**

Students at the College of Medicine have many curricular or volunteer opportunities that bring them into contact with vulnerable populations, such as children or victims of abuse, addiction, poverty, and/or low literacy, among other unnamed populations. While these opportunities contribute to the learning and development of the student as a physician who can better serve a diverse community, the inclusion of images of individuals from any potential vulnerable population in the Showcase Portfolio is strictly prohibited.

**Informed Consent as a Professional Courtesy**

Students should assume that any individual, including peers, faculty, residents, staff, or other colleagues, have a right to privacy with regards to their images. While in some circumstances taking images may be permissible by law, students should never assume consent. Ask permission before using any image as a professional courtesy. If images are not prohibited for another reason, verbal consent for use of permissible images is acceptable for use in the Showcase Portfolio.

Revised 1.27.2017
Guidelines for Use of Photography/Videography for Portfolio Artifacts

Questions

Please contact the portfolio program with questions or concerns.

Citations

1. OSUWMC Social Media Policy/Procedure. https://medcensearch.osumc.edu/sites/policies/Documents/SocialMedia.PDF
2. The Ohio State University Honor Code https://medicine.osu.edu/students/life/resources/honor_code/pages/index.aspx
6. OSUHS Consent and Authorization for Photography form.
Consent and Authorization for Photography, Videotaping, and Other Imaging For Non-Clinical Purposes

<table>
<thead>
<tr>
<th>Name</th>
<th>Date of Birth</th>
<th>MRN</th>
</tr>
</thead>
</table>

I consent to the taking, and authorize the use and publication of images (photographs, films, or videotapes) taken on ____/____/____, by which I may be identified.
These images will be used for educational purposes, including lectures, exhibits, scientific talks, presentations or papers.

This authorization is subject to the following conditions:

1. These images shall be used only for the purposes indicated above, and include the use and disclosure of the image(s) both internal and external to the Ohio State University Wexner Medical Center; **AND**
2. The authorization remains valid until the non-clinical purposes listed above are complete.
3. I may revoke this authorization, at any time, by submitting a written request that it be cancelled to the person who obtained the authorization.

I understand that:

1. I am voluntarily authorizing the taking and publication of these image(s) (photographs, films or videotapes) for the purposes listed above.
2. I can refuse to sign this consent and authorization.
3. My treatment, payment, enrollment and eligibility for benefits do not depend on my signing this authorization form. I am waiving my right to confidentiality regarding the image(s) by signing this form.
4. Once this information is released, it may no longer be protected by state or federal confidentiality laws and may be re-disclosed.
5. If applicable, I waive both ownership interest to the educational materials developed and authority to inspect or approve the finished materials prior to their release or publication.
6. By placing my signature below, I acknowledge that I understand the content of this form, and that any questions that I have regarding the image(s) or their use have been answered to my satisfaction.

Patient/Authorized Representative __________________________ Date __________

Signature of Person Obtaining Consent _________________________ Date __________

If Authorized Representative, Relationship to Patient __________________________

Printed Name of Person Obtaining Consent __________________________

Witnessed by (optional) __________________________ Date __________
DEPARTMENT OF MEDICAL INFORMATION MANAGEMENT

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Medical Record Number:

For Office Use Only

Patient Name: __________________________ Date of Birth: ______/_____/_____

Last 4 Digits of the Social Security Number: __________________________ Telephone Number: __________________________

I Authorize (check appropriate box):

☐ University Hospital  ☐ Ross Heart Hospital  ☐ OSU/Harding Hospital  ☐ Dodd Hall  ☐ James Cancer Hospital

☐ University Hospital East  ☐ Clinic  ☐ Other (please specify): __________________________

To Release Medical Information To (check appropriate box):

☐ Other Name: __________________________  ☐ The Ohio State University Medical Center

Address: __________________________ Please specify physician or department and address:

______________________________________________________________________________

Purpose of Disclosure: ☐ Medical Treatment  ☐ Disability  ☐ Insurance  ☐ Legal Reasons  ☐ Personal  ☐ Other:

Dates of Service:

Specific Reports To Be Disclosed:

☐ Emergency Department Reports  ☐ Operative Reports  ☐ Assessment

☐ Discharge Summary  ☐ Physical/Occupational Therapy Notes  ☐ Treatment Plan

☐ Laboratory Reports  ☐ Pathology Reports  ☐ Progress Notes (May Include Social Work Notes)

☐ History & Physical  ☐ Radiology Reports  ☐ Admission Note

☐ Social Work Notes  ☐ Other: __________________________

Per Ohio Revised Code 3701.741, you may be charged a fee for copies of medical records. If you have questions about copying fees please contact HealthPort at 1-800-367-1500.

I hereby authorize the treatment facility indicated above and its employees to release the designated information contained in my patient record or designated record set. I understand and acknowledge that this authorization extends to all or part of the information designated above, which may include treatment for physical and mental illness, alcohol and/or drug abuse, and/or AIDS (Acquired Immunodeficiency Syndrome), and/or may include results of an HIV test or the fact that an HIV test was performed. Information in the form of audio, photo, or video has been designated above, if applicable. A separate authorization is required for the release of psychotherapy notes. I expressly consent to the release of information designated above. This authorization is valid for 365 days, unless revoked by my written notice, provided said notice is received prior to release of the above designated information.

The revocation of this authorization is effective except as indicated in Ohio State University Health System’s Notice of Privacy Practices. Information released by this authorization may no longer be protected by federal privacy rules, such as HIPAA. I understand that Ohio State University Medical Center cannot condition my treatment or payment for health care on this Authorization unless the treatment is research-related or the care was provided solely to provide information for a third party.

X

Signature of Patient or Person Authorized to Consent Date Signed

X

Relationship, if not the patient

X

Witness (Optional) Date Signed

For records covered by 42 CFR Part 2: This information has been disclosed to you from records protected by Federal Confidentiality Rules. The Federal Rules Prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Federal Rules restrict any use of information to criminally investigate or prosecute any alcohol or drug abuse client.

MC040184 (3/10)
Policies and Procedures: Photography of Patients

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>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.</td>
</tr>
<tr>
<td>Protected Health Information (PHI)</td>
<td>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.</td>
</tr>
<tr>
<td>Protected Health Information Image (“PHI-I”)</td>
<td>Any identifiable image of a patient or procedure. These images may be stored and transmitted in various manners (see below).</td>
</tr>
</tbody>
</table>

Items that could be used to individually identify patients include, but are not limited to:

- The patient’s name;
- The patient’s Medical Record Number or Encounter Number;
- The patient’s face or any part of the face;
- The patient’s birth date, admission date, discharge date, date of death;
- The patient’s Social security number;
- 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.
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

<table>
<thead>
<tr>
<th>Subject</th>
<th>Office</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Questions</td>
<td>Security Officer</td>
<td>293-7942</td>
</tr>
<tr>
<td></td>
<td>Privacy Officer</td>
<td>293-4477</td>
</tr>
</tbody>
</table>

History

Issued: January 14, 2008
Revised: June, 2015
Submitted by: HIPAA Steering Committee
Approved by: HIPAA Steering Committee
PHOTOGRAPHY, VIDEO AND AUDIO RECORDING – CREATION, RECORDING AND STORAGE GUIDANCE

PURPOSE: This document provides guidance on the acceptable uses, unacceptable uses, and considerations to determine the appropriateness of photography, video and audio recordings of patients (“Recordings”), in the Nationwide Children’s Hospital (“NCH”) environment. **THE ENTIRE DOCUMENT SHOULD BE READ AND UNDERSTOOD PRIOR TO MAKING DECISIONS REGARDING THE USE OF RECORDINGS.**

Use of this guidance will help ensure effective compliance with NCH policy and other regulations. NCH may determine at any time that particular uses of Recordings are not appropriate in the environment.

SCOPE: This guidance applies to Nationwide Children’s Hospital (NCH) Workforce Members (as defined in IS Policy and Standard Glossary (XIV – 10A)) or others using or intending to use Recordings for any purpose.

Do not take Recordings unless supporting a legitimate business purpose approved by NCH management.
Recordings of patients generally include identifiable information and are therefore considered to be protected health information (PHI). Full face photography or videos of patient images are considered PHI. As a result, appropriate precautions such as encryption of Recordings, physical security of devices, destruction of data, de-identification of data, and appropriate process documentation must be taken to comply with HIPAA and NCH policy and procedures.

In order to ensure compliance with the appropriate policies and technical requirements associated with Recordings at NCH the following checklist is provided as guidance for current or future use of Recordings.

☐ **ENSURE APPROPRIATE CONSENT**

Prior to Recording for any purpose (including education purposes), Workforce Members must obtain consent. The General Consent form does allow for capture of photos and videos for patient care purposes, however some scenarios may require specific consent forms beyond just the General Consent form. To ensure proper consent information please contact Legal Services to review the scenario and to decide what consent forms would be appropriate.

Workforce Members **should not be included** in Recordings (Administrative Policy V-26).

If the purpose of the Recording requires Workforce Members to be present in the Recording, Workforce Members are permitted to decline being included in video. Examples include family recorded video where Workforce Members are included as they provide training, NCH marketing video projects coordinated by marketing, and recorded presentations given by staff.

Workforce Members may be recorded as a part of ongoing physical security monitoring without consent.

☐ **ENSURE SECURE RECORDING AND STORAGE OF MEDIA**

Recordings containing PHI must be stored and transported securely from the time the Recording is created until it is destroyed. Approved devices include:

- NCH provided encrypted iPod, NCH provided encrypted Phone, NCH provided encrypted laptop, or other NCH provided encrypted device;
- NCH provided encrypted USB device; and
• NCH file share location provided by Information Services.

Camera storage cards, unencrypted portable media, and portable hard drives are not likely encrypted or physically secure. In these cases, transfer the Recording to a secure device as quickly as feasible, and delete the recording from the recording device to minimize impact of a theft.

Physically secure recording equipment and storage devices used for Recordings to further secure the information.

**Personally owned phones, cameras, or other devices should NOT be used by Workforce Members to create Recordings.**

☐ **ENSURE PROPER RELEASE OF INFORMATION**

Prior to releasing Recording to any external entities, a HIPAA compliant release and authorization (MR-9 and/or AM-75) must be signed by the parent/legal guardian of the patient.

A Media Relations representative must be contacted before releasing any information to the media (including YouTube, social media, personal or corporate blogs, e-mail, or other internet sites) regarding NCH, its patients or Workforce Members.

☐ **VALIDATE APPROPRIATE SURROUNDING**

Background images in the Recording must not include non-consented patients, families, and staff.

Minimize identifying features in the Recording (i.e. when trying to photograph a wound on the arm, do not include the face of the patient therefore reducing the likelihood of identifying the patient).

☐ **CONSIDERATIONS FOR FAMILIES RECORDING THEIR CHILDREN**

NCH staff has final authority and may request families stop recording for any reason.
Families must not include patients, Workforce Members, or patient information in their Recording. Families should be asked to delete recordings if Workforce Members notice the content includes these elements.

NCH supported applications can be used to facilitate family Recordings and access to the family Recordings (i.e. NICView application).

Families assume total responsibility for their Recording equipment. Under no circumstances should NCH assume responsibility for video equipment on behalf of the family.

For the safety of our patients and staff, recording equipment must be battery operated, light sources must be contained within the recording equipment, and tripods are prohibited due to the potential tripping hazard.

☐ CONSIDERATIONS FOR VIDEO OF PATIENT USED FOR EDUCATION & TRAINING

1. If purpose is educating or training the parent, family, or patient
   - Refer to consent policy for family and Workforce Members (if applicable) (See Patient Family Care Policy – 015-030 Consent Relationships and Requirements).
   - Minimize identifiable information in the video.
   - Be aware of language and direction provided in the recording.
   - Review the video prior to releasing to the family. Use wise judgment and consider the impact if video was made public. Do not release video that would put NCH, Workforce Members, physicians, etc. at risk.
   - Do not post on web sites or other public forums.

2. If purpose is for educating or training clinical or non-clinical Workforce Members, students, researchers, or other affiliated or non-affiliated entities (conferences, course work, etc.)
   - Ensure content form is available.
   - De-identify any PHI if consent does not cover the usage. This includes metadata that could be stored on an image (location, or other image tagging).
USE ONLY APPROPRIATE RECORDING DEVICES

Approved recording devices should be used for recording and storage of Recordings containing PHI. The approved devices (currently iPod camera and/or NCH owned mobile phone) can be obtained by requesting them via the IS equipment request form located on Anchor.

Personally owned phones, cameras, or other devices should not be used by Workforce Members to create Recordings.

OBTAIN AUTHORIZATION FOR STORAGE OF RECORDINGS

The ongoing creation and storage of Recordings over time requires expensive storage space. Where Recordings will be stored, a retention period must be documented and the retention managed accordingly.

Processes that require long term storage (longer than (12) twelve months) of Recordings (lengthy video, or many videos) must be approved – approval can be obtained using the Media Storage Approval Form.

A Media Storage Approval Form (see form attached below) should be filled out and turned into HIM anytime Recordings will be stored. All Forms completed should be sent to the Director of Health Information Management.

It is not appropriate to store and transmit Recordings to internet based storage sites, YouTube, social media sites, internet video editing sites, or other internet based sites without a signed Media Storage Approval Form in place. All PHI that is captured in Recordings to be stored in such locations must be deleted, destroyed or encrypted in transit and at rest.

DETERMINE IF THE RECORDING IS CONSIDERED PART OF THE MEDICAL RECORD

Generally, Recordings are not considered to be part of the medical record. However, Recordings that are intended to become part of the medical record (used for care/treatment decisions and stored in Epic) must be reviewed by each of the following:

- Director of HIM
- Physician Department Section Chief
- Department Head or Program Manager
• Legal
• CIO

☐ REPORT INCIDENTS RELATED TO THE LOSS OF PHI INCLUDING LOSS OF RECORDINGS OR MEDIA CONTAINING RECORDINGS

Notification can be sent to the Information Security Officer, the Privacy Officer, or reported on the Corporate Compliance Hotline.

☐ IF STILL UNSURE, REQUEST HELP FROM THE RECORDING REVIEW COMMITTEE

A committee consisting of HIM, the HIPAA Privacy Officer, the HIPAA Security Officer, Legal, IS and others as required can review questions and provide further guidance. Please contact us by e-mail to “Video Compliance Recording” or vcr@nationwidechildrens.org.

RELATED DOCUMENTS:

A. Authorizations:
   http://moss/sites/HIPAA/SharedDocs/Forms/AllItems.aspx

B. Policies:
   http://anchor.columbuschildrens.net/webapplications2/DocContent/doccontent.cfm?type=Policies#33

C. Related Document Names

• Information Security and Privacy Management Policy (ADMIN XIV-3)
• Confidentiality and Technology Use Agreement (ADMIN XIV-6)
• Data Protection Standard (ADMIN XIV-3C)
• Patents and Copyright Policy (ADMIN III-5)
• Internet and Intranet Publishing Policy (ADMIN V-8)
• Publishing Guideline (ADMIN-V-8)
• Use of Social Media Policy (ADMIN-V-34)
• Use of Recording Devices and Audio/Video (ADMIN-V-26)
• Media Relations Policy (ADMIN VII-1)
• Authorization for disclosure of Protected Health Information Policy (ADMIN-XI-3)
• Disclosures to Family & Friends (ADMIN XI-9)
• Guideline for Use and Disclosure of Protected Health Information (ADMIN XI-11)
• Uses and Disclosures for Research (ADMIN XI-14)
• Uses and Disclosures for Marketing (ADMIN XI-13)
• Patient/Parent Requests for Health Information (ADMIN XI-16)
• Accounting of Disclosures (ADMIN XI-18)
• Importing Data into Epic (ADMIN XII-4)
• Consent Forms
  o MR-9 Authorization for US to Release Protected Health Information
  o AM-75 Authorization for Public Disclosure
• Media Storage Approval Form (See attachment below)
• Non Patient Care Release and Authorization consent form
• IS Policy and Standard Glossary (ADMIN XIV – 10A)
MEDIA STORAGE APPROVAL FORM

Department ___________________________________
Contact Name ______________________________
Contact Phone _____________________________

1. Please explain what specific media you are interested in retaining (i.e. photos, videos, audio recordings, electronic scans, other).

2. What is the minimum retention period for this media? Indicate timeframe (i.e. months/years).

3. Cite any state or federal laws, regulations, or requirements that support the retention timeframe you listed above (include exact citations that dictate retention requirements requested or attach actual citations).

4. Will this media be accessed by external parties/vendors, etc.? Please explain:

5. Provide estimates of volume and file sizes (i.e. We will see 5000 patients annually and need to store a 30 minute video recording for each patient).

6. Are you requesting a centralized, secure, online storage location (i.e. shared drive) to access your files?
   _____ YES or _____ NO

7. Will this media need to be attached directly to the patient’s EMR? *
   _____ YES or _____ NO

   * If yes, please complete the section below. In general we do not include media as part of the legal medical record; however, if you wish to be granted an exception please provide a business justification below.

Complete this section if media is to be attached to the patient’s Electronic Medical Record (“EMR”).

8. Explain why this media needs to be retained in the patient’s EMR.

9. Please elaborate on the location in Epic where you are requesting this media to be housed/attached (e.g. patient level, encounter level, order level, external order/result, patient ID).

{00070559 6}
10. How will the media be uploaded into Epic?

11. Describe your process for monitoring the quality and accuracy of all imported media.

12. Describe your process for monitoring the retention period and destroying data that exceeds the approved retention period. (i.e. Who will do this? What process will you follow? What quality controls will be used?)

13. Provide any other information that may be pertinent to your request.

Signature Kept on File

Signature of Department Head or Program Manager Date

All completed and signed forms MUST be submitted to the Director, Health Information Management. HIM approval is required for all EMR storage requests.

Created 1/2014