HIPAA INTERVIEW, PHOTOGRAPH AND AUDIO STANDARD

Where protected health information (PHI) is obtained, through interviews, in photographs or in audio format and is associated with services provided by covered components or for use in HIPAA-covered research, safeguards will be applied to protect the information from accidental disclosure or destruction, ensure that access to the information is appropriately limited and that authorizations are obtained, when required.

Procedure:

Non-Treatment Interviews, Photographs, or Audio

In areas at Purdue that are covered by HIPAA, execution of interviews and/or obtaining photographic images or audio of individuals that include PHI, and for purposes other than treatment, research, or for the clinical training of health care providers, must be approved by the department head(s) of the affected department(s) or designee.

The Purdue form, "Authorization for Use, Disclosure or Release of Protected Health Information" must be completed by each individual who is the subject of the PHI or their legal representative, prior to executing the interview, photo or audio recording, for purposes other than treatment or for clinic-sponsored training of covered health care providers. For example, this would include sharing of videos or audio with non-clinic faculty or class members that are not covered by HIPAA or for interviews of participants in employee wellness news articles. The authorization is not required, where a waiver of the authorization requirement has been granted by the IRB for use of PHI for research purposes. A facial image or voice print of the individual, alone, is enough identification to require an authorization. The HIPAA authorization must be filed in the patient's record, or by the HIPAA liaison or researcher, in a non-health care provider area. Care must be taken to disclose the contents of the recording only as specified in the HIPAA authorization.

Photographs, Interviews or Audio for Treatment Purposes

Photographic images, interviews or audio captured by healthcare providers strictly for treatment purposes or for use in clinical training programs sponsored by the covered component, do not require an authorization. All information captured for these treatment purposes must be stored in the patient record and will be disclosed in according to the Health and Mental Health Record Disclosures and Tracking procedures. All HIPAA policies and procedures can be accessed at: https://www.purdue.edu/legalcounsel/HIPAA/FormsProcedures.html.

Photo, Video or Audio Capture Devices and Removable Media

Devices used by Purdue workforce to capture photos, video, or audio for use by Purdue, must be properly erased prior to removing the device from the location where the media was recorded and after the data has been transferred to another secure location. PHI transferred onto removable

media must be encrypted when stored. The area HIPAA liaison, supervisor or research principal investigator is responsible for ensuring that the encryption and erasure was completed according to Purdue standard. The ITaP Security and Policy department provides standards that must be followed for proper erasure and encryption of PHI. Refer to the Communication Guidelines for HIPAA at: https://www.purdue.edu/legalcounsel/HIPAA%20forms%202020/communicationguidelines-20201.pdf.

In the case where an outside entity is recording the information on their own device and for their own purposes and where a Purdue HIPAA authorization has been obtained, authorizing the identification of a patient or health plan member associated with a covered function or activity, devices for recording video or audio will be provided by the non-Purdue entity and safeguarding of the information will be the responsibility of the receiving party.

Storing Audio or Video Media:

Videos or audio recordings of treatment sessions or patient interviews, ***used for purposes of critiquing clinician procedures, for use in research or for other non-treatment purposes***, will not be considered part of the medical or mental health record, however likely contain PHI and therefore, uses, disclosures and safeguards must be in compliance with HIPAA.

In all cases, where removable media is used for storing PHI, or electronic transmissions of PHI are needed, encryption must be used to secure the data. Refer to the Computer Security section in the HIPAA Communication Guidelines for HIPAA at https://www.purdue.edu/legalcounsel/HIPAA%20forms%202020/communicationguidelines-20201.pdf.

Media Libraries Maintained for Training Purposes and Using Removable Media

The media used for storing the recording will be encrypted, inventoried, numbered and stored in a locked cabinet located in the clinic or mental health facility. A check out form will be filled out upon removal and return of the media to ensure that the location is tracked. The form must include at least, media inventory number, date/time of removal and return, who checked out the media and use purpose. Patient identifiers should be avoided, if at all possible. These cabinets must be locked at all times and access to cabinet keys should be strictly limited.

Media should be labeled on the outside with an inventory number and listed on an inventory sheet (as described above). Additional descriptive information about the content may also be included on the media label, as needed for identification of the topic. Media should be returned to the video cabinet within 24 hours. Media should only be viewed in private areas within the clinic facility, away from where others could view the session, or in an appropriate classroom setting, as specified in the HIPAA authorization.

The video or audio recording ***must not be copied*** onto a secondary computer or other media.

Recordings Created for Treatment or Other Purposes

Recordings of treatment sessions ***used for purposes of treatment or diagnosis*** will be considered part of the patient record and maintained and tracked within that record.

If a physical patient record is maintained, removable media storing PHI must be encrypted and labeled with the patient name, date of birth and PUID or medical record number. Recordings uploaded to an electronic health record will be erased from the capture device or other removable media after successful upload.

Storage used for all PHI must be reviewed for compliance with the HIPAA Security Rule requirements and approved by ITaP Security and Policy.