Standard Operating Procedure (SOP) for Anonymizing Clinicopathology Case Conference (CPC) Videos for Educational Resource Creation

1. Purpose

This SOP outlines the procedures for scrubbing clinicopathology case conference (CPC) videos to create an educational resource while ensuring compliance with HIPAA, IRB, and institutional guidelines for patient privacy, data security, and ethical considerations.

2. Scope

This procedure applies to all personnel involved in recording, editing, and distributing CPC videos for educational and research purposes. This includes the Alzheimer's Disease Research Center (ADRC) and other centers involved in creating a National CPC Video Library.

3. Responsibilities

- CPC Organizers at each participating institution: Ensure IRB-approved protocols and legal consent procedures are followed for recording CPC sessions.
- Video Editors (TBD): Scrub videos according to HIPAA, IRB, and institutional standards, ensuring de-identification of Protected Health Information (PHI).
- Compliance Officer at each participating institution: Ensure the scrubbing process adheres to legal and institutional guidelines, reviewing final videos for compliance.
- Content Review Committee (TBD): Review scrubbed videos for educational quality and legal compliance before online resource distribution.
- Data Security Personnel at each institution: Ensure secure storage and sharing of videos, following institutional security protocols and IRB guidelines.

4. Definitions

- Scrubbing: The process of removing or anonymizing PHI from recorded CPC sessions.
- PHI (Protected Health Information): Identifiable health information, as defined by HIPAA, which includes patient names, medical record numbers, images, and other personal identifiers.
- De-Identification: The removal of all PHI to ensure compliance with HIPAA standards.

5. Procedures

5.1 Pre-Recording Guidelines

1. IRB and Legal Compliance: Ensure the recording of CPCs is covered under an IRB-approved protocol and meets HIPAA compliance. Confirm with the institutional privacy office for consistency with institutional policy. Get consent prior to death during patient enrollment and additional consent from next of kin after the individual's death.

2. Consent Process:

- Before Death: Obtain written consent from the individual at the time of enrollment. Consent should include provisions for CPC recordings and potential use in other teaching settings prospectively.
- After Death/Autopsy: Obtain additional consent from family members or legally authorized representatives. Ensure that participation or agreement to share the video is unanimous or determined by power of attorney (POA).
- Next of Kin/Surrogate Decision Makers: The more open the process is to the next of kin, the more likely it is to secure participation. Include timepoints for obtaining consent to ensure thorough documentation.

3. Consent for Genetic Information: Obtain explicit consent for sharing genetic information if included in the case discussion, to protect against potential reputational harm or privacy risks.

5.2 Recording Process

1. Recording Setup:
- Avoid capturing unnecessary audience members or patient images unless critical to the educational content.
- Ensure PHI such as location, treatment centers, or race/ethnicity is not explicitly mentioned or visually identifiable.

2. Audio Recording:
- Use clear audio to capture presenters while ensuring that all PHI spoken aloud is noted for scrubbing.
- Refrain from discussing identifiable or sensitive family information, particularly related to financial decision-making, inheritance risks, or legal matters (e.g., contesting wills).

5.3 Scrubbing Process

1. Initial Review: Review the recording thoroughly for PHI, including visual and spoken information. Mark any instances of HIPAA 18 identifiers, such as names, dates of care, and locations. Reframe dates of care as broader time points (e.g., 6 months after symptom onset) to prevent identification.

The 18 HIPAA identifiers, which must be removed to de-identify health information according to the HIPAA Privacy Rule, are:

1. Names
2. All geographic subdivisions smaller than a state (including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people)

3. All elements of dates (except year) directly related to an individual (including birthdate, admission date, discharge date, date of death, and all ages over 89, which must be aggregated into a single category of age 90 or older)
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web URLs
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographs and any comparable images
18. Any other unique identifying number, characteristic, or code (except as permitted for re-identification purposes in limited cases)

*These identifiers must be removed to consider health information de-identified under HIPAA, ensuring the individual's privacy and protection of personal health information.

* In addition, the de-identification of PHI shall also comply with the UTHSA Institutional Handbook of Operating Policies, specifically Chapter 11 Patient Privacy Policies, including but not limited to:
11.1.4 Patient Photography, Videotaping, and Other Imaging (if applicable),
11.2.9 De-Identification of Protected Health Information, and
11.2.12 Uses and Disclosures of Protected Health Information for Research.

2. Visual De-Identification:
- Scans and Images: Ensure all identifiable data on medical images or scans is removed or blurred. This is a common issue highlighted by Data Safety Monitoring Boards (DSMBs).
- Avoid references to exact locations (e.g., “patient lived in X city”), and instead, use general terms like urban or rural environments. Consider including the Area Deprivation Index (ADI) if socioeconomic or environmental context is necessary.

3. Audio Scrubbing:
- Mute or bleep patient names, specific dates, locations, or any other PHI mentioned during the session.

- Ensure that the patient's occupation, race/ethnicity, and treatment facility details are either generalized or removed.

4. Review Genetic Information: Ensure any genetic information is de-identified or anonymized, especially if the case involves familial or inherited risk factors. Genetic data should be scrutinized carefully by the participating institution's IRB office and compliance officer to avoid unintented reputational harm.

5.4 Review and Compliance

1. Internal Review: Have the scrubbed video reviewed by the Content Review Committee to confirm that all PHI is properly de-identified and the educational content is intact.

2. Compliance Check: Ensure that the Chief Compliance Officer or their designee reviews the video for compliance with HIPAA, IRB, and institutional standards. Verify that the scrubbing process is consistent with the institutional group protocol and privacy standards.

3. Consent Confirmation: Confirm that the family consent process is complete and thoroughly documented. Address any family concerns related to posthumous use and clarify the educational/research purposes of the videos.

5.5 Data Storage and Access

1. Secure Storage: Store both original and scrubbed videos in secure, encrypted environments. Institutional-approved platforms, such as [cloud-based storage services](https://www.security.uci.edu/how-to/cloud-services/), should be used to safeguard against unauthorized access.

2. Access Control: Limit access to scrubbed videos to authorized personnel, including those responsible for educational resource creation and compliance officers.

3. Embargo Periods: Implement a minimum embargo period (e.g., 3-5 years) after death to avoid potential conflicts, such as family contestations over legal or financial matters. Ensure no data is released before the embargo period without explicit next-of-kin approval.

5.6 Data Sharing and Use

1. Scope of Use: Clearly outline in consent forms whether the video will be used solely for educational purposes or if it may be used for future research, including genetic research, publications, or presentations. Re-consent will not be necessary in case new research directions or new uses for videos arise. Ensure the IRB protocol reflects the intended scope.

2. Consent for Sharing Identifiable Data: Do not include identifiable data in any shared or published videos unless explicit consent is obtained from the patient or next of kin for this purpose.

5.7 Reporting and Monitoring

1. Annual IRB Reporting: Submit annual reports to the IRB, including any issues with compliance or concerns related to data use. Ensure adherence to the institutional standard reporting and monitoring requirements for non-compliance or unanticipated issues.

2. Periodic Monitoring: Periodically review scrubbed videos to ensure continued compliance as privacy regulations and institutional policies evolve.

6. Legal and Ethical Considerations

- HIPAA Compliance: Follow HIPAA regulations regarding the de-identification of patient data and consult the HIPAA 18 identifiers list as part of the scrubbing process.
- IRB and Legal Consent: Ensure that consent is obtained from patients (prior to death) and their families or legally authorized representatives (posthumously). Engage with the privacy office and legal ethics experts to ensure the scrubbing and consent process is legally sound.

7. Document History

- SOP Created: 09/30/2024
- Last Revision: [Insert Date]
- Next Review: [Insert Date]