Contents

- Part 1: Introduction
- Part 2: Confidentiality of Clinical Trial Participant Records
- Part 3: Exceptions to Confidentiality Requirements
- Part 4: Maintaining Confidentiality of Research Participants
- Part 5: Certificates of Confidentiality
- Part 6: Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- Part 7: Permitted Disclosures of Protected Health Information
- Part 8: HIPAA Rights, Privacy, and Enforcement
- Part 9: Summary of Key Points

Part 1: Introduction

Federal regulations require that research records identifying the participant be kept confidential to the extent permitted by applicable laws and regulations. For example, if the results of a clinical study are published, participants' identities must remain confidential (45 CFR 46 ; ICH GCP 4.8.10(o)).

Federal law also protects the confidentiality of individually identifiable health information for all research participants. Other federal laws and regulations protect the records and identity of vulnerable populations as well as study participants receiving alcohol and drug abuse treatment.

This module summarizes federal laws and regulations that protect the confidentiality and privacy of study participants.

In addition to federal laws and regulations, many states have enacted their own laws and regulations to protect the confidentiality and privacy of individuals receiving health care. Researchers must be familiar with the confidentiality and privacy provisions that apply in the state where their studies are conducted.

Part 2: Confidentiality of Clinical Trial Participant Records

What records must be kept confidential?

45 CFR 46 provides protections for the confidentiality of research participants as follows:

- Subpart A – Basic protections of human research participants
- Subpart B – Additional protections for research participants that are pregnant women, fetuses, neonates
- Subpart C – Additional protections for participants that are prisoners involved biomedical and behavioral research
- Subpart D – Additional protections for research participants that are children

In addition to 45 CFR 46, the Health Insurance Portability and Accountability Act (HIPAA) mandates privacy protections for individually identifiable health information under 45 CFR 160 and 164. In general, whether research related or not, all records of the identity, diagnosis, prognosis, or treatment of any person in a clinical trial must be maintained. This includes any record in connection with alcohol or drug abuse prevention, education, training, treatment, rehabilitation, or research must be kept confidential. "Identity" includes not only the participant's name but also any other information that could be readily linked to the participant. Additionally, applicable information may be in any form (e.g., paper, electronic, verbal). The HIPAA Security Rule, also under 45 CFR 160 and 164, establishes standards to protect individuals' electronic personal health information.

For example, clinical research staff may not disclose that a participant is enrolled in an HIV study. This type of disclosure would be in violation of the participant's confidentiality and can make things difficult for the participant given the stigma associated with the disease in certain communities.

With certain exceptions, an alcohol or drug abuse treatment program may not disclose to anyone outside the program that a particular person attends the program, or disclose any information that identifies a person as an alcohol or drug abuser, unless:

- the person consents to the disclosure in writing, or
- the disclosure is allowed by a court order and the study or research site is not operating under a Certificate of Confidentiality (see Part 5 of this module for the provisions and exceptions of Certificates of Confidentiality).

A breach of confidentiality is usually defined as any disclosure of protected information about a participant to a third party without either a court order or consent of the participant. The breach of confidentiality may be oral or written and may occur by telephone, fax, or electronic means (e.g., electronic mail or other internet-based method of communication).

Part 3: Exceptions to Confidentiality Requirements

Federal regulations identify certain exceptions to the confidentiality requirements for alcohol and drug abuse participant records. Consider the following circumstances for disclosure:

“Need to Know” (42 CFR 2.12(c)(3))

Information in a participant's medical record can be disclosed to people within a health program, or between a health program and an entity having direct administrative control over that health program, as they may need this information to perform duties related to the participant's diagnosis and treatment. For example, a physician at the research site may provide participant information for the purpose of referral for treatment of alcohol or drug abuse to another health entity within the site or program.

Criminal Activity (42 CFR 2.12(c)(5))

Information in a participant's medical record can be disclosed to law enforcement officers when the participant has committed or threatened to commit a crime on program premises or against program staff.

The information disclosed must be limited to the circumstances of the incident, including the participant's:

- Participant status.
- Name and address.
- Last known whereabouts.

Suspected Child Abuse or Neglect (42 CFR 2.12(c)(6))

Information in a participant's medical record can be disclosed when it is necessary to report suspected child abuse or neglect to state or local authorities. However, original participant records may not be used in civil or criminal proceedings that arise from the report.

Armed Forces and Veterans Administration (42 CFR 2.2(e))

The confidentiality regulations do not apply to the exchange of information regarding suspected child abuse and neglect within the Armed Forces or between the Armed Forces health care facilities operated

by the U.S. Veterans Administration (VA). The regulations do not apply to the reporting of child abuse or neglect under State law.

In addition, disclosure of confidential information without a participant's consent is permitted in the situations described below (42 CFR 2.51).

Medical Emergencies (42 CFR 2.51(a))

Confidential information about a participant may be given to medical personnel in a medical emergency for the purpose of treating a condition that poses an immediate threat to the health of any person and requires immediate medical intervention.

Research Activities (42 CFR 2.52)

Confidential information about a participant may be disclosed for research purposes, provided that the recipient of the information:

- Is qualified to conduct the research.
- Has a research protocol that ensures the information will be kept secure and will not be re-disclosed except to the source from which it was obtained.
- Will not identify any individual participant in any report of the research.

In addition, a group of at least three independent persons must review the protocol to ensure that:

- The rights and welfare of participants will be adequately protected.
- The risks of disclosing information about participants are outweighed by the potential benefits of the research.

Audit and Evaluation Activities (42 CFR 2.53)

Confidential information about a participant may be disclosed for management audits, financial audits, or program evaluation activities provided that the information:

- Is not re-disclosed except to the source from which it was obtained.
- Is used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activity as authorized by a court order.

Danger to Self (42 CFR 2.51; 45 CFR 164.512(j)(4))

If a participant speaks of an intention to kill himself or herself, the participant must be evaluated by a qualified mental health professional. If the participant is found to be at risk for suicide, confidential information may be disclosed to ensure his or her safety. Specifically, it may be necessary to admit the participant to a hospital or to notify an emergency response team.

A member of the research team who suspects a participant is in danger of harming himself or herself should notify a supervisor, qualified counselor, or physician.

Danger to Others (42 CFR 2.51; 45 CFR 164.512(j)(4))

If a participant speaks of an intention to harm another person, he or she must be evaluated by a qualified mental health professional. If the threat is considered credible, a report must be made both to the police (42 CFR 2.12(c)(5)) and to the identified target. A member of the research team who suspects a participant

is in danger of harming another person should notify a supervisor, qualified counselor, or physician.

Communicable Diseases

Confidential information about a participant may be disclosed when the participant has a disease that poses a risk to public health. All states require that cases of selected communicable diseases be reported to local health authorities. Since 1999, certain infectious diseases have also been designated as notifiable to the National Notifiable Diseases Surveillance System (NNDSS) of the U.S. Centers for Disease Control and Prevention. However, state reporting to the NNDSS is voluntary. All states generally report the internationally quarantinable diseases (e.g., cholera, plague, yellow fever) in compliance with the World Health Organization's International Health Regulations.

State, local, or institutional policies may also require that communicable diseases be reported to other agencies. Researchers should contact their state health departments to obtain current and complete information about communicable disease reporting requirements in individual states.

Court Order

Disclosure of confidential information about a participant may be authorized by a court order if the disclosure is:

- Necessary to protect against a threat to life or a threat of serious bodily injury (e.g., child abuse, neglect, and threats against third parties) (42 CFR 2.63(a)(1)).
- Necessary to the investigation or prosecution of a serious crime (e.g., homicide, rape, kidnapping, armed robbery, and assault with a deadly weapon) (42 CFR 2.63(a)(2)).
- Relevant to a legal or administrative proceeding in which the participant offers evidence that pertains to the confidential disclosure (42 CFR 2.63(a)(3)).

A court order alone does not compel disclosure of confidential information. A subpoena or other legal mandate must be issued to compel disclosure.

Requirements of State Law

States may determine additional exceptions to the requirements for confidentiality of alcohol and drug abuse participant records. In some states, health care providers must report suspected domestic violence to authorities. Members of the research team should be familiar with their state's laws and regulations. Copies of relevant state laws should be on file at each study site.

When the research is protected by a Certificate of Confidentiality (CoC), research participants must be informed of the conditions that the certificate does not prevent disclosure. The CoC conditions for disclosure are not all inclusive of the circumstances mentioned above. (See Part 5 of this module for more information on Certificates of Confidentiality.

Part 4: Maintaining Confidentiality of Research Participants

Maintaining the Security of Written Records

When not in use, written records covered by the confidentiality regulations must be kept in a secure room, a locked file cabinet, a safe, or other secure place. Each program must adopt written procedures to control access to and use of these records.

What happens to participant records when a program is discontinued?

If a research site discontinues operation or is acquired by another program, there are certain medical record responsibilities that must be followed regarding the clinical records. Each site Principal Investigator must be aware of the procedures and retention period requirements for medical and study related records established by the sponsor and regulatory entities with oversight authority. For example, in the Clinical Trials Network, when a program is discontinued, the sponsor requires the program director to notify NIDA immediately to discuss the retention of any essential source documents created during the clinical study from which study data were obtained. Additionally, these documents must be kept at the study site, at the site, or by the sponsor, for a period defined by the sponsor.

Medical Record Responsibilities

The program must purge participant-identifying information from its records or destroy the records unless:

- The subject of the records gives written consent to transfer of the records to the acquiring program or to any other designated program.
- The law requires that the records be kept for a specified period.

Retained records must be sealed in envelopes or other containers and:

- Sealed in envelopes or other containers.
- In accordance with 42 CFR 2.19(b)(1), labeled as follows:

> "Records of [insert name of program] required to be maintained under [insert citation to

statute, regulation, court order, or other legal authority requiring that records be kept] until a date not later than [insert appropriate date]."

- Held by a responsible person who must destroy the records as soon as is practicable at the end of the specified retention period.

Recommended Routine Practices for Maintaining the Confidentiality of Research Participants

Researchers ordinarily use information that study participants have disclosed or provided voluntarily (i.e., with their informed consent) for research purposes. Because the relationship between researcher and study participant is based on trust, it is most important to ensure that the confidentiality of this information is maintained.

The following routine practices are recommended to ensure the confidentiality of research participants:

- Substitute codes for information that identifies the participant (e.g., use numbers instead of names to identify participants).
- Remove face sheets that contain identifiers, such as names and addresses.
- Properly dispose of all paper documents that contain identifiers.
- Limit access to all data that identifies participants.
- Educate research staff on the importance of maintaining confidentiality.
- Store paper records in locked cabinets.
- Assign security codes to computerized records.

Part 5: Certificates of Confidentiality

What is a Certificate of Confidentiality?

A Certificate of Confidentiality provides an additional level of protection for the privacy of participants in biomedical, behavioral, and clinical research studies.

Certificates of Confidentiality may be granted for studies collecting information that, if disclosed, could have adverse consequences for study participants or damage their financial standing, employability, insurability, or reputation. By protecting researchers and institutions from being compelled to disclose information that would identify research subjects, Certificates of Confidentiality help achieve the research objectives and promote participation in studies by assuring confidentiality and privacy to participants. For more information review the NIH Certificate of Confidentiality Kiosk.

Key Points about Certificates of Confidentiality

- A Certificate of Confidentiality is not transferable from one researcher to another.
- Every Certificate of Confidentiality has an expiration date. If the research project covered by the certificate will not be completed by the expiration date, the researcher must submit a written request for an extension well in advance of the expiration date.
- The Certificate of Confidentiality must be amended if significant changes occur in the research project (e.g., changes in key personnel, major changes in the scope or direction of the research protocol, changes in the drugs administered or the persons administering them). Amendment of the certificate must be requested in writing, giving details of the changes, before the changes are implemented.
- For a multi-site trial, one Certificate of Confidentiality (CoC) may be required for all sites. However, each study investigator may contact the CoC coordinator with the agency issuing the certificate.

Applying for a Certificate of Confidentiality

Certificates of Confidentiality are granted by the Department of Health and Human Services (DHHS). (Click here for more information and instructions about applying to NIDA for a Certificate of Confidentiality.)

Additional Information Required

The following additional information is required in the application for a Certificate of Confidentiality for any research project involving the administration of investigational product:

- Identification of the drugs to be administered; description of the methods of administration, including dosages.
- Evidence that the persons administering the drugs are authorized to do so.
- For controlled drugs, a copy of the research project's Drug Enforcement Administration (DEA) registration form.

What Participants Should Know About a Certificate of Confidentiality

Participants must be told that a research project has been granted a Certificate of Confidentiality. They must be informed that:

- Except under certain conditions, researchers may not be compelled to identify research participants in any civil, criminal, administrative, legislative, or other proceeding.
- The certificate is not transferable.
- The certificate has an expiration date.
- The certificate must be amended if major changes occur in the research project.

Part 6: HIPAA Privacy Rule

What is the HIPAA Privacy Rule?

The U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191) in 1996 to improve the efficiency and effectiveness of the health care system. The law includes provisions requiring the Department of Health and Human Services (DHHS) to adopt national standards for electronic health care transactions. Congress recognized that the introduction of advances in electronic technology into the health care system could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of federal privacy protections for individually identifiable health information under 45 CFR 160 and 164.

DHHS issued the HIPAA Privacy Rule — also known as the Standards for Privacy of Individually Identifiable Health Information — to put into operation these privacy protections. It establishes for the first time a set of national standards for the protection of certain health information. The Privacy Rule became effective on April 14, 2003. It is enforced by the DHHS Office of Civil Rights.

This section provides a brief overview of the main provisions of the HIPAA Privacy Rule. For additional information, go to HIPAA Privacy Rule and Its Impact on Research, a website created to inform the research community about the Privacy Rule.

To whom does the HIPAA Privacy Rule apply?

The HIPAA Privacy Rule applies to covered entities. A covered entity is defined as.

- A health plan.
- A health care clearinghouse.
- A health care provider who transmits any health information electronically in connection with transactions such as claims, benefit eligibility inquiries, and referral authorization requests. Providers who use a billing service or other third party to handle such transactions are also considered covered entities.

What information is protected by the HIPAA Privacy Rule?

The HIPAA Privacy Rule protects all individually identifiable health information that is held or transmitted by covered entities and their business associates. The information may be in any form (e.g., paper, electronic, verbal). The Privacy Rule calls this information protected health information (PHI).

Part 7: Permitted Disclosures of Protected Health Information

Covered entities may use or disclose the “minimum necessary” amount of protected health information (PHI) to or among themselves, without the individual's authorization, for purposes of treatment, payment, and health care operations.

The only exceptions to the “minimum necessary” requirement are for the use and disclosure of PHI:

- To or by health care providers for treatment purposes.
- To the individual who is the subject of the protected health information.
- To the Secretary of Health and Human Services, who has authority for the Privacy Rule.
- Use or disclosure that is required by the law.

Additionally, covered entities may disclose PHI for certain “public policy” purposes without the individual's authorization. However, they are required to track these disclosures for accounting purposes.

Public Policy Purposes

The HIPAA Privacy Rule permits covered entities to use or disclose protected health information (PHI) without the individual's authorization for the following public policy purposes:

- When the disclosure is required by law.
- For public health activities (e.g., prevention or control of disease, notification of adverse drug events).
- In cases of abuse, neglect, or domestic violence.
- For health care oversight activities authorized by law or regulations.
- For judicial and administrative purposes (e.g., a court order, subpoena, or warrant).
- To a law enforcement official for law enforcement purposes.
- To a coroner, medical examiner, or funeral director when the information concerns a deceased person.
- For cadaveric organ, eye, and tissue donation.
- For research purposes.
- To avert a serious threat to health or safety.
- For national security or intelligence activities.
- For workers' compensation purposes.

Permitted Disclosures of Protected Health Information for Research Purposes

Research is defined as “any systematic investigation designed to develop or contribute to generalizable knowledge.” Covered entities can disclose protected health information (PHI) when:

Authorization is Obtained from the Participant

Under the HIPAA Privacy Rule, a research participant may authorize a covered entity to use and disclose his or her protected health information (PHI) for research purposes. The authorization form must be approved by the relevant Institutional Review Board or a Privacy Board.

IRBs and Confidentiality

In accordance with the Belmont Report, IRBs must ensure adequate provision is made to protect subjects' privacy and maintain the confidentiality of data.

Protection of Subjects' Privacy.

The IRB must consider whether the research involves an invasion of privacy. Factors to be considered include:

- The private or sensitive nature of the information sought,
- The likelihood that subjects will regard the study as an invasion of privacy,
- The importance of the research, and
- The availability of alternative ways to conduct the study.

Confidentiality of Data

IRBs must evaluate whether adequate provisions exist to safeguard the confidentiality of information that is collected.

Authorization for disclosures is obtained routinely from participants during the informed consent process. The authorization may be combined with the Informed Consent Form that a research participant signs when agreeing to participate in a study, or the participant may sign a separate authorization form. In either case, the authorization must include the following:

All members of the NIDA Clinical Trials Network (CTN) must ensure that the process of obtaining informed consent from research subjects not only conforms to federal, state, and local regulations but also respects each individual's right to make a voluntary, informed decision.

- Description of the information to be disclosed.
- Identity of the person who may use or disclose the information.
- Identity of the person to whom the information will be disclosed or by whom it will be used.
- Purpose of the use or disclosure.
- Length of time the data will be retained with identifiers.
- Expiration date of the authorization.
- A statement of the participant's right to revoke authorization.
- A statement that information disclosed in accordance with an authorization may no longer be protected by the Privacy Rule.
- Participant's signature and date of signature.

Treatment programs do not need to keep track of disclosures that are authorized by the participant. In other words, once a program obtains a participant's permission to disclose his or her PHI, there is no need to document each occasion that a disclosure is made.

Sharing a Limited Data Set

A covered entity may enter into a data use agreement to use and disclose protected health information (PHI) that is included in a limited data set without obtaining either authorization or a waiver of authorization. Limited data sets may be used or disclosed only for purposes of research, public health, or health care operations.

The following identifiers are permitted in a limited data set:

- Admission, discharge, and service dates.
- Birth date.
- Date of death.

- Age.
- Geographical subdivisions (e.g., state, county, city, precinct, zip code).

The data use agreement must:

- Identify who is permitted to use or receive the limited data set.
- Stipulate that the recipient will:
    - Not use or disclose the information other than as permitted by the agreement or required by law.
    - Use appropriate safeguards to prevent the use or disclosure of the information except as permitted in the agreement.
    - Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement.
    - Not identify the information or contact the individuals whose information is included in the limited data set.

De-Identifying the Health Information

Covered entities may "de-identify" protected health information (PHI) by removing all individually identifiable health information from the record or file. Once health information has been de-identified, it is no longer considered PHI and therefore is not subject to the HIPAA Privacy Rule.

Individually Identifiable Health Information

Under the HIPAA Privacy Rule, individually identifiable health information includes the following:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a 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.
    - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile (fax) numbers.
6. Electronic mail addresses (e-mail).
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 universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the

Privacy Rule for re-identification.

Obtaining a Waiver of Authorization for Certain Research Activities

An Institutional Review Board or Privacy Board may waive, in whole or in part, the requirement that the participant authorize the disclosure of protected health information (PHI) if it is satisfied that:

- The use or disclosure involves no more than minimal risk to the privacy of individuals because
  - An adequate plan exists to protect health information identifiers from improper use and disclosure and to destroy identifiers as soon as practicable; and
  - Adequate written assurances have been provided that the PHI will not be reused or shared with any other person or entity, except as required by law, for authorized oversight of the research study, or for other research purposes.
- The research could not practicably be conducted without the waiver or alteration.
- The research could not practicably be conducted without access to and use of the PHI.

Privacy Board

A Privacy Board is a review body that may be established to act upon requests for a waiver or an alteration of the authorization requirement under the Privacy Rule for uses and disclosures of protected health information (PHI) for a particular research study. A Privacy Board may waive or alter all or part of the authorization requirements for a specified research project or protocol. A covered entity may use and disclose PHI without authorization, or with an altered authorization, if it receives the proper documentation of approval of such alteration or waiver from a Privacy Board.

For more information about Privacy Boards and the HIPAA Privacy Rule, go to Privacy Boards and the HIPAA Privacy Rule.

Preparing a Research Protocol

Covered entities may use and disclose protected health information (PHI) without authorization if the researcher states in writing that:

- The use or disclosure is solely for the purpose of preparing a research protocol;
- No PHI will be removed from the covered entity's location; and
- The PHI sought is necessary for the research.

The Participant is Deceased

Covered entities may use and disclose protected health information (PHI) without authorization if:

- The researcher states in writing that:
  - The use or disclosure sought is solely for research on the PHI of deceased persons;
  - The PHI sought is necessary for the research; and
  - The covered entity obtains documentation of the death of the persons whose PHI is sought.

Rights of Research Participants Under the HIPAA Privacy Rule

The Privacy Rule defines two new rights for research participants.

Right to an Accounting

Participants have a right to ask researchers for an accounting of their protected health information (PHI) that has been obtained under a waiver of or exception to the HIPAA Privacy Rule. An accounting of such disclosures may be requested for the previous six years.

A researcher is not required to account for disclosures that were:

- Authorized by the participant;
- Contained in a limited data set; or
- Released as de-identified data.

Other instances where accounting is not required include for national security or intelligence purposes, and disclosure to correctional institutions or law enforcement officials.

Right to Revoke Authorization

Participants have the right to revoke their authorization of the use or disclosure of their protected health information (PHI). However, the revocation has no effect if the researcher has already made a disclosure in accordance with the participant's original authorization.

Enforcement and Oversight of the HIPAA Privacy Rule

The DHHS Office of Civil Rights is responsible for enforcing compliance with the HIPAA Privacy Rule and for investigating complaints about lack of compliance. Failure to comply with the Privacy Rule may result in the levying of civil or criminal penalties. For more information about enforcement of the Privacy Rule, go to http://www.hhs.gov/ocr/hipaa/.

Part 8: HIPAA Rights, Privacy, and Enforcement

Interactive: HIPAA, Privacy, and Enforcement

A breach of confidentiality is usually defined as any disclosure of protected information about a participant to a third party without either a court order or consent of the participant. The breach of confidentiality may be oral or written and may occur by telephone, fax, or electronic means (e.g., electronic mail or other internet-based method of communication).

Users are instructed as follows:

There are five scenarios described below. Based on the scenario, classify whether there was a breach of confidentiality by choosing *Breach* or that there is no breach of confidentiality by choosing *No Breach*.

Scenario 1

An investigator completed a clinical trial and later published on the results of the study. A researcher for another study read the publication and contacted the study's investigator to request the data sets, with de-identified participant data, for secondary analyses. The study's investigator shared the de-identified data sets with the researcher.

Feedback: How would you classify this scenario: Breach or No Breach? The correct response is No Breach. Study data may be disclosed for research purposes as long as the data shared is de-identified.

Scenario 2

A study clinician shared a participant's test results with the study physician to confirm the participant's eligibility to participate in the clinical trial.

Feedback: How would you classify this scenario: Breach or No Breach? The correct response is No Breach. Information in a participant's medical record can be disclosed to people who need this information to perform duties related to the participant's diagnosis and treatment.

Scenario 3

Mary, a 25 year old woman who is being treated as an outpatient at Mercy Hospital's Research Center, was enrolled in a clinical trial at the center. When asked to complete a HIPAA form, Mary authorized release of medical records to her general practitioner only. Mary's mother was interested in learning more about her daughter's treatment, but she did not want to confront Mary about her concern. When Mary's mom contacted the research center directly, the front office staff immediately transferred the call to the study counselor. After confirming Mary's date of birth and social security number with her mom, the study counselor explained that she understands the situation and disclosed that Mary is enrolled in a HIV clinical trial at the center. However, she cannot go into the details of Mary's treatment.

Feedback: How would you classify this scenario: Breach or No Breach? The correct response is Breach.

Clinical research staff may not disclose that a participant is enrolled in a study without either the consent of the participant or a court order along with a subpoena or other legal mandate.

Scenario 4

A study on opioid substance use disorder is being conducted at Physicians General, a local research site. The investigator has obtained a Certificate of Confidentiality over the study. Jim, a parolee, is enrolled in the study at Physicians General. Parole Officer Bridges visits the research site and demands a copy of Jim's drug test results, with a court order. The study physician releases Jim's drug test results to Officer Bridges.

Feedback: How would you classify this scenario: Breach or No Breach? The correct response is Breach. A court order alone does not compel disclosure of confidential information. A subpoena or other legal mandate must be issued to compel disclosure.

Scenario 5

Immediately after having been administered study medication, a participant is having an allergic reaction at the research site. When the ambulance arrives, the study clinician provides to the paramedics the status of the participant's emergent medical condition prior to transporting her to the hospital.

Feedback: How would you classify this scenario: Breach or No Breach? The correct response is No Breach. Information in a participant's medical record can be disclosed to people who need this information to perform duties related to the participant's diagnosis and treatment.

Part 9: Summary of Key Points

- Federal law and regulations protect the confidentiality of participant records. In addition, Federal law protects the confidentiality of identifiable health information for all research participants.
- In general, all records of the identity, diagnosis, prognosis, or treatment of any person that are maintained in connection with alcohol or drug abuse prevention, education, training, treatment, rehabilitation, or research must be kept confidential.
- The regulations identify certain exceptions to the confidentiality requirements. Information in a participant's medical record can be disclosed:
    - To people performing duties related to the participant's diagnosis, treatment, or referral for treatment of alcohol or drug abuse.
    - To law enforcement officers when the participant has committed, or threatened to commit, a crime on program premises or against program staff.
    - When reporting suspected child abuse or neglect to state or local authorities.
    - To medical personnel in a medical emergency.
    - For research purposes, with certain conditions.
    - For management audits, financial audits, or program evaluation.
    - If a participant is found to be at risk for suicide or if he or she makes a credible threat to harm another person.
    - When the participant has a communicable disease that poses a risk to public health.
    - When authorized by a court order.
    - When required by state law.
- If a program discontinues operation or is acquired by another program, there are certain medical record responsibilities that must be followed regarding the clinical records. Each site Principal Investigator must be aware of the procedures and retention period requirements for medical and study related records established by the sponsor and regulatory entities with oversight authority.
- A Certificate of Confidentiality provides an additional level of protection for the privacy of participants involved in research studies.
- Except under certain conditions, a researcher who has obtained a Certificate of Confidentiality cannot be compelled to identify research participants in any federal, state, or local civil, criminal, administrative, legislative, or other proceeding.
- Participants must be told that a research project has been granted a Certificate of Confidentiality.
- The HIPAA Privacy Rule protects all individually identifiable health information that is held or transmitted by covered entities and their business associates. The information may be in any form (e.g., paper, electronic, oral). The Privacy Rule calls this information protected health information (PHI). A covered entity may not use or disclose PHI except as permitted or required by the Privacy Rule.
- Covered entities may use or disclose the “minimum necessary” amount of PHI to or among themselves, without the individual's authorization, for purposes of treatment, payment, and health care operations.
- PHI may be disclosed for research purposes when the disclosure is authorized by the research participant. Authorization for disclosures is obtained routinely from participants during the informed consent process. Treatment programs do not need to keep track of disclosures that are authorized by the participant.
- Health information that has been de-identified by the removal of all elements that could identify an individual is no longer considered PHI and is not subject to the Privacy Rule.