

June 22, 2022

To: Human Research Protection Program Offices
Research Compliance Offices
Healthcare Compliance & Privacy Offices
Campus Privacy Officers
Contracts and Grants Offices

From: The Guidance Memo is jointly issued by the Research Policy Analysis and Coordination (RPAC) unit and Ethics, Compliance and Audit Services (ECAS).

Subject: Guidance on Certificates of Confidentiality

Purpose

This Guidance Memo provides information about Certificates of Confidentiality (CoC), which federal agencies may issue to persons engaged in research to protect the privacy of research subjects. CoCs prohibit disclosure (even in the face of a compulsory legal demand, such as via a court order or subpoena) of identifiable, sensitive research information to anyone not connected to the research, except under specific circumstances. For research studies that collect identifiable sensitive research information, CoCs are, in some cases, issued automatically by the federal agency funding the research. In other cases (for federally funded or non-federally funded research), CoCs may be issued by a federal agency upon request by the researcher.

This Guidance Memo also highlights good data management practices in cases where identifiable research information is comingled with other data, such as in the electronic medical record. Good data management practices, which incorporate safeguards to protect confidential information from unauthorized disclosure, support CoC requirements and are essential for the protection of research participants' privacy.

1. Overview

Under 42 U.S.C. §241(d), the federal Department of Health and Human Services (HHS), in coordination with other federal agencies as applicable, must (in the case of federally funded research) and may (in the case of non-federally funded research) issue CoCs to persons engaged in sensitive biomedical, behavioral, clinical, or other research, for the purpose of protecting the privacy of research subjects. When a CoC is in place, researchers and their institutions may not disclose the names of research subjects or any information, documents or biospecimens containing Identifiable Sensitive Information (ISI, see definition below) about

research subjects to anyone not connected with the research, unless one of the following exceptions are met:

- Required by federal, state, or local laws (e.g., as required by the federal Food, Drug, and Cosmetic Act, or state laws requiring the reporting of communicable diseases to state and local health departments). Notwithstanding this exception, a CoC **does** prohibit disclosure in any federal, state, or local civil, criminal, administrative, legislative, or other proceeding absent the consent of the individual to whom the information pertains;
- Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains, and the individual consents to the disclosure;
- Made with the consent of the individual to whom the information, document, or biospecimen pertains; or
- Made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research. (42 U.S.C. § 241(d)(1)(C)).

A CoC does **not** prevent a research subject from accessing information about themselves or from voluntarily disclosing ISI about themselves. However, if the intent is to limit subject access, there may be other agreements, including a HIPAA authorization for research, which may contain terms restricting release of certain ISI to a research subject to whom the data pertains.

2. Background

Congress first authorized CoCs in the 1970s to allow researchers conducting research on illegal drug use to protect the privacy of individuals who were the subject of such research by withholding the names and identifying information of such individuals from disclosure to anyone not connected with the research. In 1979, the protection was expanded to include research on mental health, as well as research on the use and effect of alcohol and psychoactive drugs. In 1988, the protection was expanded to health research generally.

More recently, the 21st Century Cures Act, passed in December 2016, expanded the scope and impact of CoCs in three ways. First, the Cures Act introduced a new term, “**Identifiable Sensitive Information**,” to refer to the types of information that a CoC protects. The Cures Act broadly defines ISI as any information about an individual gathered or used in the course of research where:

- An individual is identified; or
- For which there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of information, a request for information, and other available data sources could be used to deduce the identity of the individual. (42 U.S.C. § 241(d)(4)).

This language broadened the threshold for identifiability from “could reasonably lead to” to “at least a very small risk.” In addition, while CoCs were previously granted based on the *sensitivity*

of a study, the Cures Act tied CoCs to the *identifiability of a participant*, implying that the concept of “sensitive” information may figure less in present CoC applicability determinations.

Second, the Cures Act made the issuance of CoCs mandatory for federally funded research involving ISI. Prior to passage of the Cures Act, issuance of a CoC was at the discretion of HHS and other federal agencies to which an application was made. Now, HHS, in coordination with other federal agencies as applicable, must issue a CoC to investigators or institutions engaged in federally funded research in which ISI is collected. Some HHS agencies automatically issue CoCs for such research without prior application by the investigator. This means that institutions and their investigators together are responsible for:

- Determining whether the research they conduct involves ISI that is either:
 - Protected by a CoC automatically issued by the applicable federal agency, or
 - Eligible for protection under a CoC upon application by the researcher; and
- Ensuring that studies covered by a CoC have processes in place to facilitate compliance with CoC requirements. See Appendix A for a detailed checklist.

Third, the Cures Act strengthened privacy protections for research subjects by outright prohibiting institutions and researchers from disclosing any ISI collected during research covered by a CoC (except under very specific circumstances) to any person not connected with the research. Previously, CoCs allowed, but did not require, institutions and researchers to refuse to disclose identifying research information to those not connected with the research, unless the participant consented to such disclosure.

3. Determining If a Research Project is Covered by a CoC or If a Researcher Should Seek a CoC

Institutions and their investigators are responsible for determining whether the research they conduct is or should be protected by a CoC. That is, researchers should determine if their research project involves collection or use of ISI. If it does, and the research is funded by NIH or another federal agency that automatically issues CoCs, then the research is protected by a CoC. In such a case, the researcher and the institution may not disclose ISI to individuals not connected to the research unless an exception applies.

If the research involves ISI but is not funded by a federal agency that automatically issues CoCs, the researcher should strongly consider applying for a CoC with the applicable federal agency to help protect the privacy of subjects. Information in the next section of this Guidance Memo explains which federal agencies automatically issue a CoC at the time of award.

NIH considers research in which ISI is collected or used to include research that:

- Meets the definition of human subjects research as defined in the Federal Policy for the Protection of Human Subjects (45 CFR § 46), including exempt research in which subjects can be identified;
- Collects or uses human biospecimens that are identifiable or that have a very small risk that some combination of the biospecimen, a request for the biospecimens, and other available data sources could be used to deduce the identity of an individual;

- Involves the generation or use of individual level human genomic data; or
- Involves any information about an individual for which there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual, as defined in subsection 301(d) of the Public Health Service Act.

4. CoC Issuance

Most HHS agencies that fund research issue CoCs. Some HHS agencies issue them automatically as a term of the award while others require a researcher to apply for them. The National Institutes of Health (NIH) and Centers for Disease Control (CDC) issue most CoCs automatically. Other federal agencies, such as the Substance Abuse and Mental Health Services Administration (SAMHSA), require a direct application from funded researchers. Further detail follows.

Research Funded by NIH or CDC

CDC and NIH (including all NIH institutes and centers) automatically issue a CoC as a term of the grant or contract for most research they funded wholly or in part. This policy applies to NIH or CDC grants and contracts that started, or were ongoing, on or after December 13, 2016.

In these cases, CoCs are no longer issued in a separate document. The Notice of Award and the NIH Grants Policy Statement will serve as documentation of the CoC protection.

Food and Drug Administration (FDA)-Regulated Research

For FDA regulated research that is not funded by a federal agency that issues CoCs, FDA will accept requests for CoCs from Investigational New Drug Application/Investigational Device Exemption (IND/IDE) holders, and issue CoCs on a discretionary, case-by-case basis.

Agency for Healthcare Research and Quality (AHRQ) Confidentiality Statute

NIH does not issue CoCs for research funded by AHRQ, but AHRQ has its own confidentiality regulations which may apply and provide similar protections. Researchers working on projects funded by AHRQ that involve ISI should contact AHRQ for further information about their privacy regulations.

Department of Justice (DOJ) Privacy Certificate

NIH does not issue CoCs for DOJ-funded projects, but DOJ has its own confidentiality and privacy regulations which may apply and offer similar protections. Researchers working on projects funded by DOJ that involve ISI should contact DOJ for further information about their privacy regulations and Privacy Certificate.

Other Research Not Funded by an HHS Agency

For research funded by a non-HHS federal agency or that is non-federally funded research, researchers can request a CoC from NIH for health-related studies where ISI is collected or used. In some cases, the IRB may require the researcher to obtain a CoC as a condition for IRB

approval. Some studies are not eligible for a CoC, including those that are not research-based, do not collect ISI, or do not involve a subject matter within a mission area of the NIH.

Table of CoC Issuance by Funding Agency

| Funding Agency | Issuance | Process |
|--|---|---|
| NIH | Automatic | Applies to research involving ISI that is funded wholly or in part by NIH: <ul style="list-style-type: none"> • Grants • Cooperative Agreements • Contracts • Other Transaction Awards • NIH Intramural Research Program |
| CDC | Automatic | Applies to research involving ISI that is funded wholly or in part by CDC: <ul style="list-style-type: none"> • Grants • Cooperative Agreements • Contracts • Other Transaction Awards • CDC's Intramural Research |
| SAMHSA, HRSA, IHS | PI must apply to the agency for a CoC | Contact the Agency CoC Coordinator: <ul style="list-style-type: none"> • SAMHSA • Health Resources and Service Administration • Indian Health Service |
| AHRQ | N/A | AHRQ has its own privacy regulations that may apply. |
| DOJ | N/A | DOJ has its own privacy regulations for research that they fund. |
| Regulated by the FDA and not funded by an agency listed above | IND/IDE holder may apply to the FDA for a CoC | FDA will issue CoCs on a discretionary, case-by-case basis. See this FDA guidance document . |
| Research not funded or regulated by an agency listed above | PI may apply for a CoC to NIH | Submit request through NIH online CoC system. See: <ul style="list-style-type: none"> • How to Get a Certificate of Confidentiality • CoC FAQs |

5. Scope and Permanence of CoC Protections

The CoC protections cover all information, documents, or biospecimens containing ISI about research subjects gathered or collected by the investigator during the research, including copies that are shared for other research activities. ISI collected in another country are

protected by the CoC, if the data are maintained within the U.S. If the data are held in the foreign country, a CoC may not be effective in the foreign country, as HHS may not have the authority to enforce compliance.

The protection of the CoC is permanent. With respect to research that has been conducted under a CoC, the CoC's protection continues even after study funding has ended (often noted as the "expiration date" of a CoC) and the study has been completed. ISI collected after the CoC has expired (including for projects that were automatically issued a CoC) are not protected even if the ISI are collected from subjects who are already enrolled in the study and the study is approved by the IRB. If funding for the research has ended and the recruitment of new research participants will continue without that funding, researchers should apply request a new CoC for continuity of protections.

Since protection of the CoC is permanent, if a secondary researcher receives ISI protected by a CoC, the secondary researcher is required to uphold the protections of the CoC.

6. Significant Changes to Research under a CoC

If a significant change is made to a research project, NIH requires that researchers submit a request to obtain a new CoC. Significant changes include, but are not limited to:

- Major changes in the scope or direction of the research protocol;
- Changes in personnel having major responsibilities in the project (such as the PI); or
- Changes in the drugs to be administered (if any) and the persons who will administer them.

Adding a participating research site to a multi-site study is not a significant change and does not require a new CoC.

7. CoCs for Multi-Site Research

For NIH- or CDC-funded research, a coordinating center or lead institution may request and receive a CoC on behalf of all participating sites. The lead site is responsible for communicating CoC requirements to sub-awardees and downstream recipients of ISI. All sites, however, are responsible for complying with the CoC restrictions on ISI disclosure.

In instances when a multi-site research project is not funded by an agency that automatically issues CoCs, the lead institution is responsible for developing appropriate agreements with the participating institutions to implement CoC requirements. Alternatively, each collaborating institution may apply directly for a CoC to cover their research activities in the project.

8. CoCs and Consent Form Language

For all studies that will obtain informed consent, research participants must be informed about the protections provided by a CoC, and any exceptions to those protections (such as state mandatory reporting). The NIH provides [example consent language regarding CoCs](#).

9. CoCs and the Medical Record

ISI associated with clinical research may be included within the medical record of the research participant. As part of the consent process, participants must be informed that certain research information related to their study participation, including the research consent document, may be placed in their medical record. Participants should also be informed that information placed in their medical records may be released to medical providers, insurers, or any others not connected with the research for the purposes of care and treatment and for healthcare operations, which may include billing and payment.

To the extent that a campus places CoC-protected ISI into the medical record, each location is responsible for implementing safeguards to protect ISI covered by a CoC. Campuses should consider mechanisms for responding to the release of ISI to both outside entities and for protecting ISI directly accessed by those within the institution who are not connected to the research. To notify those responsible for responding to release of information (ROI) requests to outside entities, campuses may implement an Epic "Never Ok to Release" ROI Special Attention flag to signal that CoC-protected encounter-level information may not be disclosed. To protect CoC-covered information accessed by those within the institution, campuses may apply encounter-level Epic "Break-the-Glass" functionality. For further information on this approach, consult your campus health privacy office.

Additionally, campuses may implement the Epic Research module or other similar research-focused applications to provide a more robust set of options to segregate research information from health information required to be in the electronic medical record, as well as to facilitate CoC and related privacy compliance.

10. Enforcement Mechanisms

Each federal agency that issues CoCs has independent authority to make decisions as to requirements, standards and processes for issuance of CoCs. Each agency is also responsible for enforcing regulations and compliance with the terms of the CoC. Should an institution or a researcher not uphold the protections of the CoC, the agency that issued the CoC may open an inquiry with the institution and researcher, look for a corrective action plan, and possibly impose disallowances, penalties, or restrictions on the researcher or institution.

11. Relationship with Other Privacy and Data Protections

Health Insurance Portability and Accountability Act (HIPAA)

CoC protections apply to Protected Health Information (PHI), as defined and protected by HIPAA, if PHI is created as part of a research study. Though HIPAA permits use or disclosure of PHI in response to certain judicial or administrative orders, a CoC prohibits such disclosure. Therefore, CoCs protect researchers from forced disclosure of ISI collected or used in research that might otherwise have to be disclosed under HIPAA.

12. Institutional and Researcher Responsibilities

Institutions and their investigators are responsible for determining whether the research they conduct is or should be protected by a CoC. When a CoC applies, institutions and their researchers are responsible for the following:

- Informing study participants about the CoC, as described above in the “CoCs and Consent Form Language” section of the Guidance Memo.
- Communicating CoC requirements to sub-awardees and downstream recipients of ISI and ensuring that they are aware of their responsibilities for complying with the CoC restrictions on ISI disclosure.
- Not disclosing or providing ISI in any federal, state, or local civil, criminal, administrative, legislative, or other proceeding, or to any other person not connected with the research, unless one of the exceptions described in the “Overview” section of this Guidance Memo applies.
- Those who receive court orders, subpoenas, or other legal processes mandating disclosure of ISI protected by a CoC should immediately contact their campus counsel.
- Ensuring information protection controls are in place using the systemwide [Electronic Information Security Policy IS-3](#).

Each campus may specify additional responsibilities related to the CoCs.

References

- National Institutes of Health, “[Notice of Changes to NIH Policy for Issuing Certificates of Confidentiality](#)”. Notice Number: NOT-OD-17-109, released September 7, 2017.
- National Institutes of Health, “[Notice of Transition to New System for Issuing Certificates of Confidentiality for Non-NIH Funded Research](#)”. Notice Number: NOT-OD-20-075, released February 28, 2020.
- National Institutes of Health, [FAQs about Certificates of Confidentiality](#)
- National Institutes of Health, [How to Get a Certificate of Confidentiality?](#)
- National Institutes of Health, [Example Informed Consent Language](#)
- Food and Drug Administration, [Certificates of Confidentiality Guidance for Sponsors, Sponsor-Investigators, Researchers, Industry, and Food and Drug Administration Staff](#), November 2020.
- Centers for Disease Control [Additional Requirement – 36: Certificates of Confidentiality](#)
- [Section 301\(d\) of the Public Health Service Act](#) (42 U.S.C. 241(d))

- [21st Century Cures Act \(Cures Act\)](#) (Public Law 114-255)
- University of California [Information Security Policy and related standards](#).

Additional Information

Please see the “CoC Compliance Checklist” (Appendix A) for a list of CoC-related processes or activities to assess for compliance at your location.

Contact

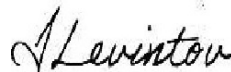
Contact RPAC if you have policy questions about the guidance provided above. Contact ECAS if you have compliance questions about the guidance provided above.

Agnes Balla
Research Policy Analysis & Coordination
Agnes.Balla@ucop.edu
(510) 987-9987

Noelle Vidal
Ethics, Compliance & Audit Services
Noelle.Vidal@ucop.edu
(510) 915-6288



Deborah Motton, Ph.D.
Executive Director
Research Policy Analysis & Coordination



Irene Levintov
Chief of Staff and Interim Systemwide
Director of Compliance
Ethics, Compliance & Audit Services

Appendix A

CoC Compliance & Best Practice Checklist

| # | Memo Section(s) | Checklist Questions | Y/N Comments |
|--------------------------|-----------------|--|--------------|
| Study Preparation | | | |
| 1 | 2-7 | <p>Are researchers (and others throughout your location who may interact with CoC-protected ISI) aware of CoC requirements and risks?</p> <ul style="list-style-type: none"> • Do researchers know when a CoC applies and when it may be advisable to apply for one to help protect privacy of research subjects? • Do researchers know how to assess whether a COC has been issued automatically to their study, or if they must apply to the appropriate federal agency for a CoC? • Does your location have a process for documenting and maintaining a record of which studies are covered by a CoC? • When significant changes are made to a project, is a new CoC sought with the issuing agency? • Are sub-awardees and downstream data recipients aware that they are subject to the requirements of the CoC? • For studies that require informed consent, are participants informed about CoC protections and any exceptions via the consent process? • Are ISI collected under a CoC maintained pursuant to CoC protections permanently? | |
| 2 | 1, 2, 8 | <p>For research covered by a CoC, do research plans specify that ISI is recorded, maintained, and transmitted in a manner that prevents disclosure and promotes privacy and security of the ISI?</p> <ul style="list-style-type: none"> • If ISI could be segregated from the EHR or other environments that are used for non-research purposes, is this considered for the study? • Are tools which support CoC compliance in Epic ("Never Ok to Release", "Break-the-Glass") or the Epic Research module considered and applied if helpful and feasible? • Where a system allows, is ISI access provisioning only made to those who need the ISI for their roles? • Is CoC protected ISI kept in officially approved secure repositories? | |

| # | Memo Section(s) | Checklist Questions | Y/N Comments |
|--|-----------------|--|--------------|
| | | <ul style="list-style-type: none"> • Is CoC protected data only transmitted via officially approved secure channels? • If the ISI collected under a CoC are classified as P3 or P4 according to the IS-3 Policy, is the project reported to the security office and recoded in inventory? | |
| Processes to Prevent Inappropriate Disclosure | | | |
| 3 | 2, 10 | <p>Do your location's release of information offices (ROI, HIM) and practices include measures to prevent CoC-prohibited disclosures such as the following?</p> <ul style="list-style-type: none"> • Disclosures in response to requests related to all federal, state, or local civil, criminal, administrative, legislative, or other proceedings? • Disclosures to any other person not connected with the research? | |
| 4 | 2, 4, 8, 11 | <p>When ISI is comingled in a multi-purpose environment (such as in the EHR), are process in place to ensure that CoC-protected ISI is not inappropriately disclosed?</p> <ul style="list-style-type: none"> • Do staff in Health Information Management (HIM), Release of Information (ROI), and other offices that release health information understand the CoC requirements and apply them correctly? • Do processes reflect the fact that CoC protections are permanent? | |
| 5 | 2, 4, | <p>Do individuals outside HIM or ROI offices who receive court orders, subpoenas, or other legal processes mandating disclosure of information protected by a CoC know to immediately contact their campus counsel?</p> | |
| 6 | 9 | <p>Are any complaints or notifications regarding CoC violations tracked and corrected?</p> | |