## 1.0 Purpose:

1.1 The purpose of this policy is to describe the obligations of the Hartford HealthCare Institutional Review Board (HHC IRB) and investigators to ensure the protection of privacy and confidentiality of information collected on human subjects for research purposes.

## 2.0 Definitions:

2.1 **Privacy** - having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. In the context of a research protocol, privacy means respecting an individual's right to be free from unauthorized or unreasonable intrusion, including control over the extent, timing and circumstances of obtaining personal information from or about them. For example, individuals may not want to be seen entering a place that might stigmatize them, such as a clearly-identified pregnancy counseling center.

2.2 **Confidentiality** – pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure without permission. In the context of a research protocol, "confidentiality" refers to the understanding between the participant and investigator (e.g., as set forth in the consent and authorization documents) as to how participant information will be handled, managed, and disseminated (e.g., shared with others) as part of the research.

2.3 **Private information -** information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record).

2.4 **Identifiable information –** information where the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

2.5 **Certificate of Confidentiality (CoC) -** CoCs are issued by the federal government [NIH, FDA and other Department of Health and Human Services (DHHS) agencies] to protect identifiable research information from forced disclosure. They allow the investigator and others who have access to research records to refuse to disclose identifying information on research participants in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. Protection against compelled disclosure of identifying information about subjects of biomedical, behavioral, clinical, and other research is provided by the Public Health Service Act §301(d), 42 U.S.C. §241(d).

## 3.0 Procedure:

3.1 **Privacy** – In meeting its regulatory requirements, the IRB must consider whether there are adequate provisions to protect the privacy interests of subjects. The IRB will consider whether a member of the research population under study would consider the information collected in the research to be private and whether the release of that information without permission would be an invasion of privacy. In order to make that determination, the IRB must obtain information regarding how the investigators are gaining access to subjects or subjects' private, identifiable information and the subjects' expectations of privacy in the situation. Investigators

must have appropriate authorization to access the subjects or the subjects' information.

3.1.1 In developing methods and strategies for the protection of subjects' privacy, consideration should be given to:

- Methods used to identify and contact potential participants
- The physical settings in which an individual will be interacting with an investigator
- Appropriateness of all personnel present for research activities
- Methods used to obtain information about participants and the nature of the requested information
- Information that is obtained about "secondary subjects", that is individuals other than the "primary subjects," and whether such individuals meet the regulatory definition of "human participant" (e.g., a subject is asked to provide information about a family member for a survey)
- How to access the minimum amount of information necessary to complete the study.

3.1.2 It should be recognized that views on privacy can vary within and across cultures and research populations. What is considered to be sensitive information by one individual may not be considered so by another. In the case that a unique culture is proposed to be studied, the IRB will request consultation from a representative of that population to provide insight as to the feelings about privacy within the culture.

3.2 **Confidentiality –** In meeting its regulatory requirements, the IRB must consider whether there are adequate provisions to maintain confidentiality of data. In reviewing confidentiality protections, the IRB shall consider the nature, probability, and magnitude of harms that would be likely to result from a disclosure of collected information outside the research. It shall evaluate the effectiveness of proposed de-identification techniques, coding systems, encryption methods, storage facilities, access limitations, and/or other relevant factors in determining the adequacy of confidentiality protections.

3.2.1 It should be noted that confidentiality and anonymity are not synonymous terms. If the identity of the subjects can readily be ascertain from the data, then the research is not anonymous and the IRB must determine if appropriate protections are in place to minimize the likelihood that the information will be inappropriately divulged. The level of confidentiality protections should be commensurate with the potential for harm from inappropriate disclosure.

3.2.2 The time of initial review, The PI will provide the information regarding the methods to maintain privacy and confidentiality of research subjects through the completion of the Research Application, any necessary HIPAA documents, research protocol, and/or other submitted, applicable materials.

3.2.3 Investigators has an obligations to ensure that the informed consent form accurately provides the subject with information concerning the confidentiality of the research records, allowing them to make his or her own determination of the acceptability of the protections offered.

3.2.4 Potential subjects should be informed, via the consent document and process, about (a) how their data will be used, (b) who will have access to their data and for what purpose (i.e. audit by federal agencies), (c) who will know about their participation in the research, (d) what methods will be used to ensure confidentiality and that unauthorized individuals will not have access to their data, (e) how long their data will be retained, for what purpose, and when it will be either destroyed or de-identified, (e) any limitations that may effect the plan to maintain confidentiality (i.e. legal reporting requirements).

3.2.5 In the case where an investigator is requesting a waiver of the documentation of consent, the subject must be provided with an information sheet that describes the plan to maintain confidentiality of their data, in addition to other required elements of informed consent.

3.2.6 Investigators requesting a full waiver of the requirement for consent and authorization must thoughtfully and sufficiently address the waiver criteria outlined in the federal regulations. These criteria include: the research involves no more than minimal risk to subjects, the research could not practicably be conducted without the waiver, and whenever appropriate, the subject will be provided with additional pertinent information after participation. The IRB will consider how thoroughly the investigator has addressed these criteria in the Research Application. One line answers are unacceptable. Because subjects have not given their explicit permission for the investigator to access their private information and it is being accessed without their knowledge under a waiver, the study team must be especially aware of keeping this information confidential.

3.2.7 The IRB shall evaluate the effectiveness of proposed de-identification techniques, coding systems, encryption methods, storage facilities, access limitations, and/or other relevant factors in determining the adequacy of confidentiality protections.

3.2.8 In studies in which the investigator proposes to collect individually identifiable sensitive information (i.e. involving illicit drug or alcohol use, genetic studies, etc.) that my place the individual at greater risk should this data be subject to judicial subpoena, the IRB may require that a Certificate of Confidentiality be obtained. (*See HRPP Policy #840 – "Certificates of Confidentiality" for further detail regarding CoCs*)

3.3 Examples of acceptable Data Security methods that may be employed to maintain privacy and confidentiality. The choice of method deemed acceptable for a given study may vary depending on whether the information is identifiable, the sensitivity of the data, potential harm to the subject should the data be lost or released to unauthorized individuals.

3.3.1 Hard copy data is stored in locked filing cabinets in locked offices. Only the PI and study coordinator have access to keys for these storage locations. Signed consent documents will be confidentially retained for at least three years; HIPAA research authorization forms will be retained for at least six years.

3.3.2 Identifiable research data, including recruitment and screening information and code keys are stored on a database located on a secure HHC network drive, which is backed-up nightly.

3.3.3 Subject identifiers and the means to link the subject names and codes with the research data are stored in separate locations within the database and with distinct access controls.

3.3.4 Access to the research database is password protected and each member of the research team is required to have a unique ID and password to gain access to the database. The PI or designated database administrator keeps a log of users with access. The IRB is notified of all members requesting access prior to granting access. Access permissions are inactivated when the study team member is no longer working on the protocol.

3.3.5 Data sets containing identifiers will not be sent through internet-based e-mail or as an attachment. If shared by e-mail, research data sets will only be sent using HHC-approved encryption (and will also be password-protected.

3.3.6 Identifiable data which is collected electronically (e.g., laptop, jump-drive, thumb drive, CD etc) is stored temporarily on the device until the identifiable data can be uploaded to the secure database.

3.3.7 Moveable electronic media used to collect or store the data is equipped with encryption software and the electronic files containing the data are also password-protected.

3.3.8 Computers used in research areas are set to lock the screensaver after 15 minutes of inactivity requiring a password to unlock the screen.

3.3.9 The PI and other members of the research team work with coded or de-identified data when using moveable device(s) to perform data analysis.

3.3.10 Moveable media devices are used to collect research data which is limited to either de-identified or collected using the subject's unique code.

3.3.11 A Certificate of Confidentiality (CoC) will be applied for through the National Institutes of Health (NIH), the US Food and Drug Administration (FDA) or the Department of Health and Human Services (DHHS) to protect subjects' privacy and ensure the confidentiality of their study data and participation in the study.

## 4.0 Documentation:

4.1 Determinations (IRB Reviewer Checklists and minutes) and any discussions related to privacy and confidentiality in a research protocol will be retained for a minimum of 6 years after completion of a study at Hartford HealthCare.

**5.0 References:**

5.1 45 CFR 46.111(a)(7) [Subpart A – *Basic HHS Policy for Protection of Human Research Subjects*]

5.2 21 CFR 56.111(a)(7)

5.3 ICH-GCP: 2.11

5.4 Institutional Review Board Management and Function, Bankert, E. A., Amdur, R. J., 2nd Edition, 2006

5.5 FDA Information Sheet – "A Guide to Informed Consent" (1998)

5.6 FDA Information Sheet – "Sponsor-Investigator-IRB Interrelationship" (1998)

5.7 Web-based learning module titled, "Privacy and Confidentiality: Current Issues in Research Ethics." http://ccnmtl.columbia.edu/projects/cire/pac/introduction/index.html

**6.0 Revision History:**

| Rev # | Initials | Effective Date | Description of Change(s) |
|---|---|---|---|
| 00 | CLB | 7/1/11 | New Issue |
| 01 | CLB | 2/2/13 | Expanded the definitions of Privacy and Confidentiality in Section 2.0; Added Section 5.8 to include internet reference |
| 02 | CLB | 3/15/20 | General review |

Element II.3.D. and II.3.E.