Section 11: Guidance for Special Topics/Procedures

11.1. What Quality Improvement and Educational/Competency Evaluation Activities are Considered Research?

There is often confusion in determining whether Quality Improvement (QI) activities fall under the jurisdiction of RSS as UIR staff are continually evaluating and improving training activities through quality assurance and performance improvement. In both situations scientific methodology is used equally. Thus, activities that require RSS review cannot be easily defined by the methods they employ. In addition, other attributes such as publication of findings, methodological design, selection of subjects and hypothesis testing and generating do not necessarily differentiate research from QI and educational evaluation activities because these attributes can be shared by both research and non-research activities. This distinction between quality improvement, education/competency activities and human subject research is challenging and evolving, and as a result we have to re-think our approach for making this distinction. The following document represents consensus that was reached by University of Illinois Rockford. It is prepared to assist investigators in determining which of their activities require RSS review.

What are the guidelines for determining whether a Quality Improvement project should be considered research and subject to RSS review?

The following principles should be used to define whether a quality improvement (QI) project should be reviewed by RSS.

- Surveys whose primary purpose is to gauge the opinions and perceptions of internal and external “customers” (trainees, staff, patients, referring physicians, and others) are an integral component of organizational quality assessment and may be considered a quality improvement activity that does not requires RSS review. Results of such surveys may yield new knowledge deserving dissemination external to the organization through presentations and publications. Therefore, surveys performed within an institution’s QI framework should not automatically require IRB consideration.
- QI projects that are designed to improve clinical care to better conform to *established/accepted standards* are not considered research.
- It may also help to think about QI as activities based on existing knowledge about the enduring nature and function of people and their environment rather than to develop new knowledge. Examples include data guided efforts to ensure adoption of evidence based on practice guideline or introduce procedures to reduce medical errors (1).

Example: Questionnaires that are distributed to UIR patients and service populations for the purpose of determining their satisfaction with a service, program or clinic and for gathering information on how to improve the service, program or clinic does not require IRB review.

What types of Quality Improvement activities require review by RSS?

The following types of studies which may be performed under the general framework of QI should be submitted for IRB review:

- Studies in which subjects or groups of subjects may be randomized to different interventions or treatments. When these interventions or treatments involve minimal risk, and particularly when informed consent would be impractical, an IRB should consider waiver or alteration of informed consent.
- Studies in which anonymity of participants cannot be assured. Participants are defined as individuals who are being asked to complete or provide feedback on a QI initiative not individuals or services that are being evaluated as part of the QI process.
- Studies involving care practices, interventions, or treatments that are not standard (neither consensus-nor evidence-based).
- Studies that involve more than minimal risk to participants.

Are there other privacy and protection issues that need to be taken into consideration even if the QI or educational/competency activity does not require RSS review?

Yes, in order to preserve privacy and mitigate sensitivity of members of the organization to adverse publicity, the following policies should be followed when RSS review is not conducted:

- Any QI or educational survey results must be completely **anonymous**, and results should be presented as aggregate data. Results must not be aggregated in such a fashion that the identity of respondents can be ascertained (e.g., identification of departments with very small numbers of staff members). Therefore, all QI surveys must contain the following language: “This is an anonymous survey. Results of the survey will be presented only as aggregate data, with complete protection of individual anonymity.”
- The survey must not be **coercive**. Individuals who do not wish to complete the survey may decline without fear of blame or punishment. Therefore, all QI surveys should contain the following language: “completion of this survey is entirely voluntary.”
- If there is any potential for publication of survey results, the survey must contain the following language: “The results of this survey may be published, using only aggregate, anonymous data. If you are concerned about publication of data from the survey and do not wish to participate, simply do not fill it out or hand it in.”

What if I want to publish my experience with either a quality improvement activity or educational/competency activity as defined above?

Intrinsic components of QI, educational initiatives, and competency assessment are shared learning. It is entirely appropriate to disseminate and replicate QI successes, including through channels that are external to an organization. This may include presentations at meetings and publications in professional journals. Therefore, the mere intent to publish the findings of a QI project does not obligate IRB review as long as the publication does not refer to the activity as research and makes it clear the publication is the result of a quality improvement or educational/competency assessment as defined above, there is no need for any action on behalf of the IRB. If a journal questions this determination, RSS would be happy to provide them with the guidelines referenced above.

Please note that these guidelines were developed to help clarify the confusion that anything that is published requires IRB review. The activities sited above do not represent all of the QI and educational activities performed at UIR. There are still some forms of QI and education research that is subject to RSS review.

Source

1. Lynn, Joanne et al. The Ethics of Using Quality Improvement Methods in Health Care, Annals of Internal Medicine 2007; 146: 666-673. http://www.annals.org/content/146/9/666.full

11.2. Guidelines for Research Funded by Department of Education and School Based Research

Policy

Any research that is to be conducted by faculty or staff of University of Illinois Rockford (UIR) in a school setting must be submitted and reviewed in accordance with UIR polices and procedures. Upon submission it may be determined that a protocol is exempt or, requires expedited or full committee approval. In reviewing research, the Committee will require that a letter of approval from the school or school system be obtained. In addition, when appropriate, investigators must comply with the Protection of Pupil Rights Amendment (PPRA) which is part of the *No Child Left Behind Act of 2001 (Public Law 107-110)* which is summarized below:

For research sponsored by the Department of Education, (34 CFR 97) research funded by the National Institute on Disability and Rehabilitation Research, when an IRB reviews research that purposefully requires inclusion of children with disabilities or individuals with mental disabilities as research subjects, the IRB will include at least one person primarily concerned with the welfare of these research subjects.

Procedures

Researchers frequently wish to conduct research in schools. Some of this research may be funded by the Department of Education which has specific requirements when using education records. Research may consists of observation in classrooms, interviews with teachers, questionnaires given to students, video or audio taping of classrooms, focus groups or interviewing parents about their children. Schools may also be used as a recruitment site for posting notices of research activities.

Approval by the Schools

The UIR IRB will request a copy of an approval notification from authorized individuals within the school or school district. Investigators are required to comply with school policies and procedures for all proposed research. Different school systems may have different procedures and the investigator is obligated to contact the school district and develop their protocol consistent with the school policies.

Is the School Engaged in Research?

If school staff, teachers, or personnel perform research procedures or release private identifiable information about students, the school may be considered engaged in research. This may include active recruitment, obtaining consent, performing research assessments or interventions. If a school is engaged in research, special considerations will need to be made as to whether the school must obtain their own IRB review or whether the schools signs an agreement to work under the jurisdiction of the UIR IRB. Schools that are only used as a site for research and permit the UIR IRB investigator to perform all the research procedures, including recruitment and obtaining consent would not be considered engaged in research.

U.S. Department of Education/Protection of Pupil Rights Amendment (PPRA), School Based Surveys and Informed Consent Requirements

The Protection of Pupil Rights Amendment (PPRA) which is a part of the *No Child Left Behind Act of 2001 (Public Law 107-110)* specifies eight categories of protected information in surveys of minors in schools. In also gives parents rights with regard to the surveying of minor students, the collection, disclosure, or use of information from students for marketing purposes, and certain non-emergency medical examinations.

PPRA has two sets of requirements for surveys. 1) requirements that apply to “protected information” surveys that are funded in whole or in part by the U.S. Departments of Education, and 2) requirements that apply to “protected information” surveys that are funded by sources other than the U.S. Department of Education and that are administered or distributed by education institutions that receive funds from any Department of Education program (i.e., public elementary and secondary schools and some private schools).

Under PPRA no student shall be required, as part of any research project, to submit without prior consent to surveys, psychiatric examination, testing, or treatment, or psychological examination, testing, or treatment, in which the primary purpose is to reveal information concerning one or more of the following categories which are considered protected information:

1. Political affiliations of student or student's parents;
2. Mental or psychological problems of student or student's family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating or demeaning behavior;
5. Critical appraisals of others with whom students have close family relationships;
6. Legally recognized privileged or analogous relationships;
7. Religious practices, affiliations or beliefs of a student or student's parents;
8. Income.

In this context prior consent means:

- Prior consent of the student, if the student is an adult or emancipated minor; or
- Prior written consent of the parent or guardian, if the student is an un-emancipated minor. Schools and contractors obtain prior written parental consent before minor students are required to participate in any Department of Education funded survey, analysis, or evaluation that are considered protected information in the categories listed above.

PPRA has implications for applying the criteria for waiving informed consent (45 CFR 46.116(d) of the Common Rule). Specifically, the second IRB criterion "research does not adversely affect the rights and welfare of subjects" is impacted because of the "rights" that PPRA gives parents.

- **First Set of Requirements U.S. Department of Education Funded Protected Information Surveys**
  - ➢ Does the research involve "protected information" surveys?
  - ➢ Are the surveys U.S. Department of Education funded in whole or in part?
  - ➢ Are the surveys "required"?

  If the answer is *YES* to the three questions, PPRA affords parents the right to provide active consent. Under the circumstance, it would be difficult to determine that the "rights and welfare" criterion for waiving informed consent entirely could be met; therefore, prior written parental consent would be required, even if the IRB determined that some of the basic elements of informed consent specified in 45 CFR 46.116(a) could be waived as inappropriate to the activity.

  Since the PPRA
- **Second Set of Requirements for Protected Information Surveys that are Funded by Sources other than the U.S. Department of Education and that are administered or distributed by education institutions that receive funds from any U.S. Department of Education administered program (i.e., public schools and some private schools)**
  - ➢ Do the surveys include protected information?
  - ➢ Are the surveys being administered or distributed by schools that receive any U.S. Department Education funds?

If the answer is *YES* to both questions, PPRA affords parents the right to inspect the surveys before they are administered or distributed, and to opt the student out of the surveys.

PPRA requires schools to develop and adapt policies, in conjunction with parents, regarding 6 areas, some of which are relevant to surveys:

1. Right to inspect a survey before administered or distributed;
2. Arrangements to protect student privacy in the administration of a survey;
3. Right to inspect any instructional material used as part of educational curriculum;
4. Administration of physical examinations or screenings;
5. Collection, disclosure or use of personal information for purposes of marketing or selling;
6. Right to inspect any instrument in the collection of information for marketing or selling the surveys.

PPRA also requires local educational agencies to notify parents of the policies and to offer parents the opportunity to opt out of (remove child from) participation in third-party surveys involving protected information. These requirements suggest that local schools have the discretion to set up their own individual policies for non- U.S. Department of Education protected information surveys. For example, local schools can choose whether to have an active written consent policy or some other policy such as passive consent. The UIR IRB will have to decide how they will handle these requirements in those protocols where the investigators are requesting passive consent. For example, the Committee might require that if an investigator asks for passive consent procedures, that he/she must also document that the procedures are consistent with the policy of the local school(s) to be included in the research sample. The IRB then can use that information in determining if the "rights and welfare" criterion for waiving informed consent has been met.

U.S. Department of Education Contact: The Family Policy Compliance Office is the office charged with administration of PPRA. Note as of May 26, 2004, the web page has the old version of PPRA. However, the Family Policy Compliance Office has released guidance documents about how No Child Left Behind revises PPRA which are on the web site. http://www.ed.gov/offices/OM/fpco/ppra/parents.html

Research Sponsored by the Department of Education Involving Student Education Records

For research sponsored by the Department of Education involving student education records the following: in order to obtain records the University of Illinois Rockford, must enter into a written agreement with the educational agency or institution that specifies the following:

- The purpose, scope, and duration of the study and the information to be disclosed.
- That the University uses personally identifiable information from education records only to meet the purposes or purposes of the study as stated in the written agreement.
- That the study will be conducted in a manner that does not permit personal identification of parents and students by anyone other than representatives of the University with legitimate interests.
- That the University is required to destroy or return all personally identifiable information when no longer needed for the purpose of the study and specifies the time period in which the information must be returned or destroyed.

11.3. Certificates of Confidentiality Guidance

What is a Certificate of Confidentiality?

A Certificate of Confidentiality helps researchers protect the privacy of human research participants enrolled in biomedical, behavioral, clinical, and other forms of sensitive research. Certificates protect against compulsory legal demands, such as court orders and subpoenas, to identify information or characteristics of a research participant.

What kind of research is eligible for a Certificate?

Any research project that collects personally identifiable, sensitive information, and that has been approved by an Institutional Review Board (IRB), is eligible for a Certificate. The NIH or other federal funding is not a prerequisite for a Certificate.

What is meant by sensitive information?

Sensitive information includes, but is not limited to, information that relates to sexual attitudes, preferences, or practices; information that relates to the use of alcohol, drugs, or other addictive products; information that pertains to illegal conduct; information that, if released, might be damaging to an individual’s financial standing, employability, or reputation within the community, or that might lead to social stigmatization or discrimination; information that pertains to an individual’s psychological well-being or mental health; and genetic information or tissue samples.

Who may apply for a Certificate of Confidentiality?

Any person engaged in research in which sensitive information is gathered from human research participants (or any person who intends to engage in such research) may apply for a Certificate of Confidentiality.

Is NIH required to give all who apply a Certificate of Confidentiality?

No. No project is entitled to a Certificate; its issuance is discretionary.

How long does a Certificate's protection last?

Individuals who participate as research subjects (i.e., about whom the investigator maintains identifying information) in the specified research project during the period the Certificate is in effect are protected permanently.

What is the researcher's responsibility to participants regarding a Certificate of Confidentiality?

When a researcher obtains a Certificate of Confidentiality, the subjects must be told about protections afforded by the Certificate and any exceptions to those protections. This information should be included in the informed consent form, unless the research subjects are not longer actively participating in the project. In addition, researchers may not represent the Certificate as an endorsement of the research project by the Department of Health and Human Services, or use it in a coercive manner when recruiting subjects.

When should one apply for a Certificate?

Inasmuch as IRB approval of a research project, or approval conditioned upon issuance of a Certificate of Confidentiality, is a prerequisite for issuance of a Certificate, in general, an application for a Certificate of Confidentiality is submitted after the IRB responsible for its review approves the research project. Since the informed consent form should include language that describe the Certificate and any voluntary disclosures specified by the investigator, the applicant may tell the IRB that he or she is applying for a Certificate of Confidentiality and has included appropriate language in the informed consent form. Applications for Certificates should be submitted at least three months prior to the date on which enrollment of research subjects is expected to begin.

Who does one contact to apply for a Certificate of Confidentiality?

If NIH funds the research project for which a Certificate is sought, application may be made through the funding Institute. However, even if the research is not supported with NIH funding, one may apply for a Certificate through the NIH Institute or Center that funds research in a scientific area similar to that of the projects. Contact information is available on the NIH website at: http://grants1.nih.gov/grants/policy/coc/index.htm

11.4. Guidelines for Using the Internet to Conduct Research Activities

Policy

This section is designed to assist investigators in addressing the appropriate ethical and practical considerations necessary for protecting human subjects when the Internet is used for research related activities. The Internet has become an increasingly popular and convenient tool for conducting research; however, it has also raised important questions regarding associated risks. This guidance document focuses on the unique issues related to collection of data over the Internet, particularly through the use of online surveys.

Procedures

How is the Internet used for research related activities?

The main categories of Internet use for research are 1) recruitment, 2) observation of Internet activities, and 3) collection of data.

Use of Internet for Recruitment

UIR IRB and approval of clinical trial listings on the internet are not required when the system format limits the information provided to basic trial information, such as the *title; Purpose of the study; protocol summary; basic eligibility criteria; study site location(s); and how to contact the site for further information*. Examples of clinical trial listing services that do not require UIR IRB approval include the National Cancer Institute's Cancer Clinical Trial Listing (PDQ), Clinicaltrials.gov, and the government sponsored AIDS Clinical Trials Information Service (ACTIS). However, when the opportunity to add additional descriptive information is allowed by the database system, the UIR IRB must review and give approval.

What do I need to consider if I want to observe Internet activities/chat rooms as part of my research protocol?

While there is presently no specific guidance from the UIR IRB on research utilizing the observation of Internet activities, or participation in chat room activities, investigators are encouraged to contact Research Support Services to discuss any issues and concerns related to such research procedures early in the protocol submission process.

Can all surveys performed as part of research utilize the Internet?

No. It is important to note that not all types of research involving surveys are good candidates for online data collection. For example, a questionnaire that may provoke anxiety or emotional distress may not be suitable for the Internet environment. It is important to consider that when research is conducted entirely through the Internet, it is not possible for researchers to assess a subject's reaction to the research, as is possible in more traditional face-to-face- or even telephone survey design. The IRB will review protocols that use the Internet on a case-by-case basis to determine whether the procedures outlined are appropriate for the nature of the research.

Likewise, if the inadvertent disclosure of research information could cause significant harm or embarrassment to subjects, the use of the Internet to conduct the research may not be appropriate. The primary source of risk in Internet research is the inappropriate breach of confidentiality, as it is impossible to guarantee the security of data transmitted over the Internet.

Do I need to be concerned about whether the subject population has access to computers/Internet and the ability to use computers/Internet?

Yes, it is necessary to consider that discrepancies in access to computers and the Internet exist, and that some individuals will be excluded from Internet based research that otherwise may have been able to participate. Investigators must address the bias introduced by conducting research over the Internet in their protocols.

What criteria will the IRB use when evaluating surveys performed over the Internet?

When conducting survey research on the Internet, researchers must adhere to the same basic ethical principles as required in any type of research. However, the use of the Internet for collection of data introduces additional concerns that must be taken into consideration by the investigator in designing a protocol and by the IRB in its review of the protocol. The IRB will use the same criteria normally used to review research protocols, as Internet-based research must offer the same level of protections of human research subjects as research that is conducted through more traditional methods. Additionally, the IRB will review the research to be sure that additional risks specifically related to Internet activities are minimized.

Data Collection and Transmission

What do I need to consider about the authentication of a subject before data collection?

Researchers need to keep in mind that there is no way to be sure that a respondent to an Internet survey is over 18 or the person the investigator seeks to involve. This is important both scientifically and for the protection of human subjects. It will be important for researchers to have a way to authenticate the identity of the subject responding to the survey. When designing protocols, researchers should consider different methods of authentication. The IRB will consider whether the authentication of subjects is appropriately outlined in a research protocol. If data resulting from a project is not valid, any potential risk to subjects may not be justified.

Are there any special issues I need to consider regarding the voluntary nature of answering individual questions on an Internet survey?

Yes. When traditional paper surveys are used, the IRB requires that subjects are given the option of skipping any question that they do not wish to answer. This option is also a requirement for surveys conducted over the Internet. When researchers design Internet-based surveys, they should include the option for subjects to skip a question and move on to the next one. Completion of any individual question cannot be forced through the use of Internet technology. A screen should also be included at the conclusion of the survey that gives subjects the option of either submitting or recalling their responses.

What do I need to consider regarding the electronic transmission of data? Do I need to have data encrypted?

Yes, security during the transmission of data from the participant’s computer to the Web server should be ensured by using a server that employ’s encryption technology. Encryption should also be utilized when the Web server is a different machine than the one on which the data will be analyzed. Researchers need to specify in their protocols the steps that will be taken to ensure the security of data stored and transmitted using the Internet.

Are there special considerations if I want to notify a subject about a study via email?

Yes, the following considerations need to be taken into account when email is used to transmit data or to provide potential subjects with information about a research study:

- Investigators should be aware that email is not a secure communication mechanism. Furthermore, a subject’s email account may be shared with another individual, such as a spouse or family member, or may be monitored by an employer. For these reasons, researchers should not include any sensitive information or the title of a study in emails, if the title itself can reveal sensitive information. Investigators also have a responsibility to inform subjects that some email accounts may be less secure than others. Subjects can take this information into account when choosing which email address to provide to researchers.
- An email may be mistakenly sent to a wrong address. Researchers should take steps to be certain that the email address is correct to be sure emails are received by the appropriate person.
- Precautions should be taken to ensure that subjects will not inadvertently respond to an email that is sent to a study listserv. The blind carbon copy function should be used so subjects cannot view the names of other participants and to ensure that a participant does not respond to all recipients of an email.
- Email should not be used to collect data; instead, investigators can send an email including a link to a secure site, where data can be collected.

- All emails should include instructions such as, "if you have received this email in error, please contact____ at the University of Illinois Rockford.

Data Storage and Disposal

Are there special requirements for data storage?

Yes, the investigators need to include in their protocol a description of how long the data will be kept and whether it will ever be destroyed. It is important to recognize that copies of electronic data/files are often kept for back-up and security purposes and therefore it may not be possible to state that data will be destroyed.

Other requirements to follow:

- Laptops and computers containing files with research data should be password protected, and individual files should be password protected as well. This is good practice for any research utilizing electronic files.
- Personally identifiable data should be stored separately from research data.
- Extra precautions must be taken when private health/identifiable information is collected. PHI must be stored on an ISD server or an ISD approved server. Data that is collected as part of a research protocol which initially includes any of the HIPAA identifiers may not be placed on any personal use device, including home computers, PDAs, smartphones, etc.

Informed Consent via the Internet

Can I obtain informed consent via the Internet?

For some protocols, the IRB will allow consent to be obtained via the Internet. The investigator must provide rationale as to why it is not practicable to obtain the subject's written signature on a consent form. In accordance with the regulations pertaining to informed consent, the researcher will need to request a waiver of written informed consent, or to request that consent is obtained through a method other than written consent. Researchers must also consider authentication of the age of subjects if individuals less than 18 will be asked to complete a survey via the Internet.

Are there specific ways the IRB would recommend I consider obtaining consent for an Internet survey?

If obtaining consent through a method other than a written consent form, one option for obtaining informed consent over the Internet is to have the first page of a survey consist of an information sheet/consent form. Then subjects can be required to check a box indicating their consent before beginning the survey. If a waiver of written consent is not granted, researchers may consider having subjects download a consent form and sign a printed copy to mail to the researcher. After receipt of the consent form, the research would provide the subject with a PIN to access the survey.

Are there special requirements for what needs to be included in the consent for surveys conducted on the Internet?

Yes. In addition to the standard information that must be included in all consent forms, investigators need to include the following information in consent forms/information sheets for online research.

- A statement that information transmitted over the Internet can never be completely anonymous and that confidentiality in Internet research can never be completely guaranteed.
- The steps that will be taken to ensure the security of data stored and transmitted over the Internet.
- Information associated with the subject that will be attached to a survey (IP address, email address, etc.).
- Contact information for the investigator, so the potential subject can ask questions.

Commerical Web Survey Vendors vs. Internal

Can I use a commercial web survey vendor?

The UIR IRB does not ban the use of commercial survey vendors, but it is required that vendors meet a minimum standard to ensure that UIR research subjects are given adequate protection. Investigators are responsible for acquiring all of the information listed below and for including it as part of the protocol application. Once the information is reviewed and found to be acceptable we hope to publish a list of acceptable vendors so that other investigators will be made aware of them and do not need to repeat collection of the same information.

1. What security measures are in place to protect data during transmission from the browser to the Web server, and during transmission to the researcher’s computer? Does the organization use Secure Sockets Layer (SSL) technology?
2. What security measures are in place to protect data stored on the Web server?
3. What does the organization do with the information it gathers about site visitors?
4. How long are log files kept?
5. Is data received date and time stamped?
6. What are the organization’s data storage and back-up policies and procedures?
7. What are the organization’s privacy and confidentiality policies?
8. Who in the organization has access to the data being gathered and stored?
9. What happens to the copy of the data file the organization has (from the back-up) when the research project is finished?

10. Who in the organization is available if other questions arise?

11.5. Research Involving Department of Defense Funding

Scope and Applicability

This information and guidance applies to all human subject's research involving the Department of Defense (DoD). Research is considered to involve the DoD when:

1. The research is funded by a component of DoD.
2. The research involves cooperation, collaboration, or other type of agreement with any component of DoD.
3. The research uses property, facilities, or assets of a component of DoD.
4. The subject population will intentionally include personnel (military and/or civilian) from a component of DoD.

Background

In the past few years, DoD has significantly enhanced their human subjects protection requirements, including the application of those requirements to researchers who are not employees of the DoD. As necessary and requested by DoD, UIR will sign an Addendum to its Federalwide Assurance (FWA). This document requires that UIR apply DoD regulations and policies for the protection of human research subjects when conducting, reviewing, approving, overseeing, supporting, or managing human subjects research involving the DoD. DoD directive 3216.2 provides the University with the additional DoD requirements.

Principal investigators (PI) will need to include in their protocol the additional information required so that the IRB may take into consideration the additional DoD requirements and determinations. DoD will require documentation of IRB approval, the risk level, and the expiration date of the research to the DoD Component of sponsoring or supporting the study. The DoD may also request additional documentation to verify compliance with federal and DoD policies, including minutes related to the research, any exemption determinations, or documentation of continuing approval. The DoD applies the provisions in 45 CFR 46, Subparts B, C, and D for the protection of vulnerable populations of subjects, but prohibits the use of prisoners of war in DoD sponsored research. Research that involves greater than minimal risk requires appointment of an independent research monitor. In certain cases, the DoD also applies limitations on the waiver of informed consent.

Definitions

Research Involving a Human Being as an Experimental Subject

An activity for research purposes where there is an intervention or interaction with a human being for the primary purpose of obtaining data regarding the effect of the intervention or interaction (32 CFR 219.102(f), reference (c)). Examples include, but are not limited to, a physical procedure, a drug, a manipulation of the subject or subject's environment, the withholding of an intervention that would have been undertaken if not for the research purpose.

DoD Components

Refers collectively to the organizational entities within the DoD that are subject to the human subjects protections laid out in the Department of Defense Directive.

Research Monitor

Refers to a physician, dentist, psychologist, nurse, or other healthcare provider designated to oversee a specific protocol that involves more than minimal risk, especially issues of individual subject/patient management and safety. The research monitor functions independently of the research team and shall possess sufficient educational and professional experience to serve as the subject/patient advocate.

Specific Considerations and Procedures

1. **Scientific Review**
   DoD requires scientific review prior to IRB review for all new DoD supported human research. Review by the Departmental scientific review committee prior to IRB submission would meet the DoD requirement. DoD also requires that all substantive amendments (see Section 6.5) to approved DoD research involving human subjects receive scientific review prior to IRB review.
2. **Education Requirements**
   DoD requires initial and continuing mandatory education requirements for human subjects protection. The UIR requirements for mandatory and continuing education meet this requirement (see Section 4.3).
3. **Research Monitor Required: Greater than Minimal Risk Studies**
   For DoD sponsored research involving greater than minimal risk to subjects, the DoD requires appointment of an independent research monitor. The research monitor has the authority to: 1) stop a research study in progress; 2) remove individuals from the study; 3) take any steps to protect the safety and well-being of subjects until the IRB can assess the research monitor's report. The PI in coordination with the IRB identifies a candidate for the position of research monitor, taking into account the nature and disciplinary focus

of the study and the likely type of medical expertise required. The IRB also ensures that the research monitor is independent of the research team.

4. **Waiver of Consent and Exception from Informed Consent in Emergency Medicine**
   If a research subject meets the definition of "experimental subject," DoD regulations prohibit the waiver of consent unless the PI obtains a waiver from the Secretary of Defense. The IRB may waive the consent process if the research does not meet the definition of "experimental subject." DoD regulations prohibit an exception from informed consent in emergency medicine research unless the PI obtains a waiver from the Secretary of Defense.
5. **Multi-Site or Collaborative Research Requirements**
   Any investigator developing a proposal for DoD funding or other support that involves other collaborating institutions needs to consult the sponsoring DoD Component and the RSS Specialist to identify additional requirements for multi-site research. Formal agreements may be necessary to ensure that participating institutions understand and accept their scope of work specific roles and responsibilities of each party are agreed upon.
6. **Provisions for Research-related Injury**
   The PI is responsible for informing the IRB if there are any requirements from DoD Component's the *provision of care in the case of a research-related injury*. If the DoD Component has stricter requirements than 45 CFR 46 (Common Rule) or UIR policies this will need to be disclosed in the informed consent document.
7. **Research Involving U.S. Military Personnel as Research Participants**
   If any research includes U.S. military personnel as subjects the IRB protocol must include a plan for research subject recruitment that incorporates additional safeguards to minimize undue influence from individuals within a potential subject's chain of command. The PI is required to consult with the sponsoring DoD Component to determine appropriate recruitment plans. In addition, unless military personnel are on leave status during research participation, they may not receive compensation for their participation.
8. **Under No Circumstances Shall the IRB Approve Research Involving Prisoners of War, as defined by the Specific DoD Component.**
9. **Additional DoD Review Required Prior to Initiation of Study**
   After the IRB completes its review and issues approval, the PI will need to submit documentation of IRB approval, the risk level, and the expiration date of the research to the DoD Component sponsoring or supporting the study. The DoD may also request additional documentation to verify compliance with federal and DoD policies, including minutes related to the research.

The PI may not initiate the study until the human research protection officer within the sponsoring DoD Component reviews and approves the IRB approval and other submitted documentation.

If the study is for DoD sponsored survey research or survey research within the DoD that involves DoD personnel, including military personnel, an additional level of DoD review of the study may be required. Surveys typically require DoD Survey Review and approval. The PI submits surveys and all required documentation relevant to survey research review to the requesting DoD Component.

11.6. Research Data Security

Policy

University of Illinois-Rockford (UIR) researchers must ensure that research data is protected, at a minimum, in a manner consistent with human subject protection regulations (45 CFR 46, 21 CFR 50 and 56), and as applicable the HIPAA Privacy and Security Rules (45 CFR 160 and 164), 2009 HITECH Act, other federal and state laws, and University policies. University of Illinois-Rockford PHI may only be used or disclosed for research purposes as described in the HIPAA authorization and as approved by the UIR IRB.

The research protocol and corresponding protocol application must include a data security and management plan. A data security/management plan should address the following:

- How data will be collected and recorded
- The type of identifiers linked to the research data
- How the data will be stored and secured, including paper and electronic formats
- If and when identifiers will be removed (data de-identified)
- Disposition or storage of data after study completion
- Any future use of the research data

This policy focuses on the data security requirements and the minimal standards for the collection, storage, use, transmission, and destruction of UIR PHI associated with research data to meet these federal mandate and institutional policies, including University Information Security policies. However, these data security standards will be similarly applied by the UIR IRB to research involving other types of sensitive and high sensitive information.

Research data consisting solely of de-identified health information do not meet the definition of PHI and therefore is not subject to the HITECH Act breach notification requirements.

Encryption of PHI or destructions of the media containing the PHI following the procedures stipulated in the statutes are the only methods recognized by the HITECH Act as rendering data into a form where it is unusable, unreadable, or indecipherable to unauthorized individuals and obviating the need for breach notification. Data is considered “secured” after encryption or destruction.

A limited data set as defined under HIPAA that excludes both date of birth and ZIP Code is also not subject to the breach notification requirements. While the data is still considered “unsecured PHI” in this instance, the HITECH Act considers such a dataset to not pose a significant risk of financial, reputational or other harm. The breach does, however, need to be reported to the IRB for record keeping purposes.

Procedures

Definitions

Data Encryption

Encryption is the conversion of data into a form, through use of an algorithm, which renders electronic data, unusable, unreadable, or indecipherable by unauthorized persons. Decryption is the process of converting encrypted data back into its original form, so the data can be usable and understood.

Protected Health Information (PHI)

Individually identifiable health information transmitted or maintained in any form or medium, including oral, written or electronic. Individually identifiable health information relates to an individual’s health status or condition, furnishing health services to an individual, or paying or administering health care benefits to an individual. Information is considered PHI where there is reasonable basis to believe the information can be used to identify an individual. ePHI: Electronically Protected Health Information.

De-Identified Health Information

Health information that does not identify an individual, and there is not reasonable basis to believe that the information can be used to identify an individual, is considered de-identified. In accordance with the HIPAA Privacy Rule, health information can be de-identified by two means:

1. *Statistical Method:* An independent statistician:
   - Determines that the risk of re-identification of the data, alone or in combination with other data, is very small; and
   - Documents the methods and results by which the health information is de-identified, and the expert makes his/her determination of risk.
2. *Removal of All Identifiers (Safe Harbor Method):* The removal of all 18 HIPAA elements from the health information that could be used to identify the individual or the individual’s relatives, employers, or household members.

The de-identified health information may include a code (re-identification code) that will permit the information to be re-identified, if necessary, provided that; the key to such a code is not accessible to the researchers requesting the use or disclosure of the de-identified health information; that the code was not derived from or related to information about the individual or cannot be used to identify individuals; and the covered entity does not use or disclose the code for any other purpose, and does not disclose the mechanism for re-identification.

Security Breach A situation in which unencrypted PHI or sensitive information is reasonably believed to have been acquired by an unauthorized person, including an employee's and/or student's access of HPI that is not in accordance with the job responsibilities, and that poses a significant risk of financial, reputational, or other harm to the individual whose records were accessed. A suspected security breach means that this information may have been lost or stolen, accessed in an unauthorized fashion or infected by a virus or worm, but it is not yet known whether the information has been compromised to meet the level of a security breach.

The HIPAA Breach Notification Rule defines a "breach" as the acquisition, access, use or disclosure in a manner not permitted under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

Exceptions to the definition of breach are described at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Sensitive/Highly Sensitive Information As defined by the September 2009 Interim UIC Information Security Policy, sensitive information is defined as information that if disclosed or modified without authorization would have severe or serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information in this category includes, but is not limited to:

- Assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, such as credit card information
- Covered by federal and state legislation, such as HIPAA, FERPA, or the Data Protection Act
- Payroll, personnel and financial information

In the research setting, sensitive information also includes individually identifiable information involving:

- AIDS, sexually transmitted diseases, or alcohol or substance abuse or treatment
- Illegal conduct or arrest records
- Sexual attitudes, preferences, or practices
- Psychological or mental health information
- Disclosure of information outside of research that could reasonably

cause discrimination or stigmatization, or result in damage to subject’s financial well-being, employability, or reputation.

Unsecured PHI PHI that is not rendered usable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specifically involving the encryption of data that are at rest (i.e., residing in databases) and/or data in motion (i.e., wireless transmission).

Collection, Storage, Use, and Transmission of Research Data with PHI and Other Sensitive Information

1. In addition to federal human subject protections regulations, electronic research data containing PHI must both be used and stored in a HIPAA compliant fashion. The HITECH Act Breach Notification Guidance identifies IT security technologies and methodologies that if used render PHI unusable, unreadable or indecipherable to unauthorized individuals.
2. The research protocol and protocol application, including applicable appendices, must describe the security measures in place for maintaining the privacy of the subjects and confidentiality of the data.
3. Only the minimum necessary PHI and other sensitive information should be collected to achieve the purposes of the research. The protocol and protocol application should describe exactly what identifiable data elements will be collected.
4. The UIR IRB expected investigators to have in place one or more of the following standards when their research data contains PHI. The IRB will determine the level of security for each protocol based on the presence of identifiers, sensitivity of the data and risks of a breach.
    a. Electronic PHI (ePHI) hosted on any device that is potentially exposed to theft or loss, including laptops, desktops, and portable devices (including but not limited to portable hard drives, flash drives, USB memory sticks, smart phones, mp3 players or similar storage devices) must be encrypted. No notification is required if a breach occurs.
        i. Encryption software applications should preferably be supported by the UIC Academic Computer and Communications Center (ACCC), and allow central management with a central key repository with a password recovery mechanism and contain auditing functions. For encryption software applications other than those supported by ACCC, the investigator must provide the IRB with documentation confirming the software’s compliance with the HITECH Act standards.
        ii. Because electronic portable devices are particularly susceptible to loss or theft, the storage of identifiable subject data, even encrypted files, should

be limited and data transferred to a secure system as soon as possible. When not in use, electronic portable devices must be securely stored.

b. ePHI hosted on servers secured and housed in a HIPAA compliant environment. Currently an example of such a server at UIC meeting these criteria is the UIMC server. For example, PHI collected from Gemini for a chart abstraction could be securely stored on the UIMC H drive. Notification is required if breach occurs, e.g., the server is hacked and unsecured PHI is removed.

c. Record and retain only de-identified data. The IRB will require documentation that investigators will not have access to identifiers or a code linked to identifiers, and will not attempt to identify the subjects. No notification if breach occurs.

d. Restrict PHI to a limited data set, where identifiable elements are limited to city, state ZIP Code, elements of date, and other numbers, characteristics, or codes not considered as direct identifiers. When additionally ZIP Code and data of birth are not contained in the limited data set, breach notification is not required. While the data is still considered “unsecured PHI” in this form, the HITECH Act considers such a limited dataset to **NOT** pose a significant risk of financial, reputational, or other harm. The breach does, however, need to be reported to the IRB for record keeping purposes. Notification may be required if the breach involves a limited data set containing ZIP Code or date of birth and the covered entity determines the breach poses a significant risk of financial, reputational, or other harm.

e. When encryption, de-identification, or a limited dataset are not able to be implemented, research data should be coded and identifiers removed by the PI or a research team member as soon as possible, with a master list containing the identifiers secured and kept in a separate file cabinet(s) (paper records) or on a separate physical device (electronic data).

5. Access to identifiers should be limited to authorized research personnel and be physically secured throughout the conduct of the research.

   a. Any paper records should be stored in a locked cabinet or other fixture in a secure location with access limited to research personnel. All personnel must be listed on the protocol application or Appendix P, and have met UIR’s human subject protections training requirements.

   b. The consent forms/authorizations should be kept separately from the data files.

6. Identifiers should be removed/destroyed as soon as they are no longer needed. The protocol should specify plans for retention or destruction of identifiers/de-identification. Once research data are de-identified, they are no longer PHI and. Therefore, no longer subject to the HIPAA HITECH Act notification requirements.

7. PHI and other sensitive research information should only be transmitted over secure networks, regardless of location, or as encrypted data files over public networks. Unless encrypted, PHI should not be e-mailed. If the research involves electronic transmission of PHI and other sensitive information, the types of transmission and methods to secure

the data during transmission must be described in the research protocol and IRB application.

8. Telefaxing of PHI for research purposes is **NOT** permitted.
9. PHI and other identifiable information, including contact information, cannot be distributed outside UIR without the specific authorization of research subjects and approval by the IRB.
10. Upon completion of the research study and submission of the *Final Report*, the investigator must describe the final disposition of all research data. If identifiers must be retained in the data files because of specific needs of this research study or anticipated future research use, the investigator must provide a justification. The IRB will expect that data be destroyed or the investigator must specify a long-term plan for maintain the security of the data, including the identity of the individual/entity that is designated as the custodian of the data.
11. Investigators leaving the employ of UIR who desire to remove the data generated from their research are required to obtain a *Data Use Agreement, Material Transfer Agreement*, or equivalent in accordance with University requirements. Additional requirements may apply regarding the removal of PHI.

    Upon the departure of an investigator, custody of data remaining at UIR must be established and communicated to the IRB. Faculty sponsors must ensure that PHI or other identifiable information is not removed in an unauthorized manner by their students, fellows, or residents.
12. The principal investigator and research team members are responsible for working with their IT administrators to ensure computers are updated with appropriate basic security measures such as anti-virus, anti-spyware, and firewall software, as well as the latest software and operating system patches.

Destruction and Disposal of PHI

1. Documents that contain PHI must be shredded before disposal or disposed of through a University approved document destruction service. Documents or materials that contain identifiers and that cannot be shredded should have the identifiers obscured or obliterated before disposal. Documents or materials with subject identifiers should never be put in the general trash.
2. Electronic media must be cleared, purged, or destroyed such that PHI cannot be retrieved and in accordance with National Institute of Standards and Technology NIST Special Publication 800-88.

Breaches of Data Security

1. To fulfill the HIPAA HITECH breach reporting requirements, any breach or suspected breach involving UIR PHI in the custody of the principal investigator, co-investigator(s),

research staff, students, or business associate should be immediately reported to the Director of Healthcare Compliance and Risk Management: 815-395-5642 schust@uic.edu.

2. Breaches or suspected breaches of data security, including PHI and other sensitive information, are considered by UIR policy to meet the definition of a potential unanticipated problem and must be reported to the IRB using the *Prompt Reporting Form* within 5 business days of becoming aware of the event. The IRB will review the report and contact the Director of Healthcare Compliance and Risk Management. Examples of possible data breaches include, but are not limited to, the following:
    - Lost or misplaced files, folders, etc.
    - Lost or stolen computer, laptop, or other electronic storage device with unencrypted PHI
    - Access of PHI without a *business* need to know (i.e., workforce access of PHI of friend or celebrity)
    - Faxes sent to the wrong fax machine
    - Improper disposal of paper containing PHI (i.e., not shredded)
    - Information delivered to the wrong participant using the postal service, courier, or other delivery method
    - Loss/violation of the integrity of decryption key or process
    - Compromised computer/device (i.e., infection by a worm or virus)
3. Investigators are strongly encouraged to immediately report breaches and suspected breaches of data security to the College/Department/IT administrator and follow applicable IT incident reporting polices.