If the original Initial application/protocol did not include advertising for the research subjects, the research investigator must submit a Modification in Cayuse IRB and provide for review all recruitment materials and methods for dissemination of the materials. The use of the recruitment materials/methods may not begin until IRB review and approval is provided.

iv. Recruitment Utilizing Clinical Trial Websites

Clinical trial websites provide a significant opportunity not only to recruit subjects, but also to foster informed consent by increasing the amount of information that is available to an individual interested in a clinical trial. The websites, such as the National Cancer Institute or CancerNet, can often generate a large number of site visits by individuals wanting to learn more about clinical trials. In some cases, the information provided on these websites may constitute the earliest components of the informed consent process.

When information posted on a clinical trial website goes beyond directory listings with basic descriptive information, such information is subject recruitment therefore requires IRB review and approval. The basic descriptive information includes title, purpose, protocol summary, basic eligibility criteria, location(s), and contact information. Information included beyond these basic listings will require review and approval by the IRB. For complete guidance, please see the OHRP guidance at http://www.hhs.gov/ohrp/policy/clinicaltrials.html. FDA guidance mirrors these principals and can be found at http://www.fda.gov/oc/ohrt/irbs/toc4.html#recruiting.

IRB review and approval of listings of clinical trials on the internet is not required for listing services such as the National Cancer Institute listing, the government-sponsored AIDS Clinical Trials Information Service, Clinicaltrials.gov, etc. However, if you plan to add additional descriptive information that is beyond the listing, IRB review and approval is required.

F. Payment Arrangement among Sponsors/Organizations, Investigators and Others

Payment in exchange for referrals of potential subjects (finder's fees) and payments designed to accelerate recruitment tied to the rate or timing of enrollment (bonus payments) is generally unacceptable. It is impermissible to accept bonus payments. The Institution's physicians and employees cannot accept personal payments from sponsors or other researchers in exchange for accelerated recruitment or referrals of patients.

10.2 INTERNET AND SOCIAL MEDIA

A. Using Internet and Social Media to Conduct Research Activities

The internet has become an increasingly popular tool for conducting research and recruiting subjects. Computer- and internet-based methods of collecting, storing, utilizing, and transmitting data in research involving human subjects are developing at a rapid rate. As these new methods become more widespread in research, they present new opportunities for potential enhancement of the dissemination of surveys, obtaining informed consent, subject tracking, and direct participation, while also presenting new compliance challenges to the protection of research subjects. The purpose of this chapter is to guide investigators in addressing the ethical and practical considerations needed for protecting human subjects when

using the internet for research activities including data collection, online surveys and interacting with subjects for research-purposes. The guidelines are comprised of requirements and recommendations that are consistent with the basic IRB principles applied to all research involving human subjects.

The IRB believes that computer- and internet-based research methodology must address fundamentally the same risks (e.g., violation of privacy, legal risks, and psychosocial stress) and provide the same level of protection as the more traditional non-electronic methods of research involving human subjects. All protocol submissions reviewed by the IRB, including those using computer and internet technologies, must:

i. Ensure that the procedures fulfill the principles of voluntary participation and informed consent.

ii. Provide rationale that supports the necessity of utilizing the proposed technology or platform.

iii. Maintain the confidentiality of information obtained from or about human subjects, to the extent that is possible given the nature and use of the platform utilized in the study. This includes the method and location(s) of data storage and accessibility of all study data (e.g. storage on local servers, third-party servers, or cloud-based storage). In addition, adequate plans to avoid collection of PHI or personal identifying information (PII) over the internet without verification of secure transmission and prior consent and authorization must be provided. The protected health information (PHI) from a social network site could lead to privacy, confidentiality, and potentially HIPAA concerns.

iv. Adequately address possible risks to subjects including risks of participation directly related to the specified technology utilized. The use of third party applications or platforms in the research must be fully vetted for privacy and confidentiality risks to subjects, including describing the limits and use of user-data proposed by such third parties. The use of data and activity on the third party platform must be disclosed to subjects and if applicable, the Terms of Use or End-User License Agreements that subjects may be required to accept in order to participate may be requested by the IRB for review.

v. The management plan in place to monitor content, information, comments, etc. if the platform or application allows for community member-generated content that will be used for research-purposes and can be accessed by other subjects enrolled in the study. For example, if the research study utilizes an online community where subjects can post communications about their participation in a clinical trial, the investigator must include a plan for monitoring posts and provide an action plan to address specific scenarios and/or remove information (such as when a subject discusses an adverse event). All communications provided and received within these interactive platforms are presumed to public may be directly identifiable. Some platforms utilize monikers (or avatars) in place of names, while others require real names. Communications should be monitored to ensure that users are not intentionally or unintentionally prompted to provide sensitive information that may affect their rights or welfare and a plan should be in place to remove, correct, or attribute any such communication.

vi. Meet the regulatory and ethical criteria for approval.

B. Online Recruitment

Computer- and internet-based procedures are increasingly being used by investigators for advertising and recruitment of study subjects. In addition, new technologies have emerged that allow direct contact with potential subjects within public and private networks. Such technologies, such as social media, forums, and group/population messaging platforms and applications allow investigators to interact directly potential research subjects.

i. Non-interactive Recruitment Accessible via the Internet

When reviewing recruitment materials that will be published on non-interactive media on the internet, the same principles apply as the more traditional non-electronic methods of subject recruitment as described above. IRB review is required for the language and content of this recruitment material published on non-interactive media.

ii. Interactive Recruitment and Social Media

Social media is a computer-mediated platform that allows the creation, sharing, and exchange of information, ideas, and pictures/videos in virtual communities and networks. These platforms can be either public or semi-private in which membership must be sought. When recruiting subjects for research using social media or other interactive platforms, there are additional responsibilities and requirements that investigators are to consider and apply in order ensuring that basic principles of research protections are maintained. When social media or another form of interactive media is used for recruitment purposes, the investigator is to provide in the Cayuse IRB Initial Application:

a. The name of all sites/applications/platforms that will be utilized
b. The content of the post that will be published on the website/application/platform that meets the requirements for recruitment as outlined above.
c. If the social media site is governed by an administer (i.e. for private or semi-private sub-groups within the social media site/application), permission has been obtained from the administrator and the groups policies and rules will be upheld
d. The name and owner of the account from which the recruitment will be posted. This includes the explanation if the post will be made from the investigator's personal account or one that is maintained by the Institution. Adequate justification must be provided if the investigator wishes to post from a personal account.
e. Confirmation that the frequency of each post is kept to the minimum number of posts necessary to achieve exposure.
f. The plan to monitor replies, sharing, and "likes" of recruitment posts and answering questions to posts; which includes confirmation from investigators that persons who share or comment to posts will not be directly solicited/contacted for direct recruitment and that questions are responded to with a statement that indicates who that person can contact to have this question answered directly. In addition, if the investigator plans to delete comments or replies to interactive posts, information will be requested on the applicability of this monitoring and the lines of authority for this editing. Investigators and other members of the study team must not "tag" specific individuals in posts or replies/comments.

g. Assurance from the investigator that if any PHI or other PII is posted in response to recruitment posts that this information will not be collected for part of the study data.

C. The Inclusion of Minors in Online Research and Recruitment

The Children's Online Privacy Protection Act (COPPA), effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

COPPA applies to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. COPPA also cover other types of information - for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms - when they are tied to individually identifiable information.

Before collecting, using, or disclosing identifiable personal information from a child, an investigator must obtain verifiable parental consent from the child's parent. This means an investigator must make reasonable efforts (taking into consideration available technology) to ensure that before identifiable personal information is collected for research purposes from a child, a parent of the child provides permission. In-addition, re-consent of parent's will be required when the terms of data collected for research purposes has changed from the original research plan.

The full description of the provisions and requirements of website operators for compliance with COPPA that can be found at http://www.coppa.org/comply.htm.

D. Online Surveys

The IRB reviews protocols that propose to use the Internet on a case-by-case basis to determine whether the use of the Internet is appropriate. When developing a survey that will be conducted via the Internet, it is important to recognize that not all types of surveys are appropriate candidates for online data collection. A survey that requests highly sensitive information or one that may cause emotional distress or anxiety may not be suitable for the Internet. When conducting surveys via the Internet, the researcher and subject do not have the benefit of the face to face, in person experience.

A risk of collecting data via the Internet is the disclosure of information that could cause significant harm or embarrassment to the subjects. The most common source of risk is the breach of confidentiality, as it is not possible to guarantee the security of the data transmitted over the Internet.

In designing a study where the Internet is used, the PI needs to consider the subject population and their access to computers so as not to exclude individuals who may otherwise be able to participate. It might be appropriate to offer the survey both electronically and on paper so as not to introduce bias in the subject sample population.

Investigators are advised that authentication - that is, proper qualification and/or identification of respondents - is a major challenge in computer- and internet-based research and one that

threatens the integrity of research samples and the validity of research results. If the respondent population is not the population that is originally targeted by the research, the resulting data may not reflect what the research was originally intending to assess. Researchers are advised to take steps to authenticate respondents. For example, investigators can provide each study subject (in person or by mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer- and internet- based data collection. For research that excludes minors, the IRB may ask the researcher to describe the procedures to be employed to authenticate that the subjects are adults. Some options are using Internet monitoring software or using Adult Check systems that can screen out minors.

E. Informed Consent Process for Online Survey-based Research

The IRB has developed an informed consent template for online survey research that should be included when developing consent forms and the consent process for online surveys. See the IRB website for additional information. For some protocols, the IRB will allow the consent for surveys to be obtained via the Internet.

IRB requirements pertaining to informed consent and disclosures for conducting online survey research include:

i. Internet consent documents and/or disclosure should be written like a cover letter and should include all the required elements consent, including the confidentiality disclaimer given below. The consent form or disclosure statement should include a method for subjects to indicate whether they agree to participate in the survey. For example, the consent form can include a statement that states, "I want to take part in this research and continue with the survey" and include check boxes for the subject to indicate yes or no. Other Internet-based surveys include "I agree" or "I do not agree" buttons on the website for subjects to click their choice of whether or not they consent to participate.

ii. The following statements are required to be included in the consent form or in the disclosure statement:

   a. A statement that lets subjects know that information transmitted over the Internet can never be completely anonymous and confidentiality cannot be completely guaranteed. For example, the consent form or disclosure statement could state, "Confidentiality will be maintained to the degree permitted by the technology used. Your participation in this online survey involves risks similar to a person's everyday use of the Internet."

   b. "If you have any questions about the research methods, you should contact the principal investigator, *(name)*, or colleagues *(identify who)* by contacting *(telephone number or e-mail address)* during a workday or *(telephone number)* at night or on weekends. Direct questions about your/your child's rights as a research subject to the Vice President and Chief Operating Officer of the Research Institute (*identify name, and contact information).*

iii. The consent must disclose that if a subject completes an anonymous survey and then submits it to the investigator, that the investigator will be unable to extract anonymous data from the database should the subject wish it withdrawn.

iv. Unless completion of an entire survey is a requirement of participation, internet-based survey instruments should be formatted in a way that allows subjects to skip questions if they wish or provide a response such as "I choose not to answer." At the end of the survey, there should be buttons that give subjects the option to discard the data or to submit it for inclusion in the study. If completion of an entire survey is a requirement of participation, the consent document must clearly state this requirement and remind prospective subjects that they may choose not to participate or can stop participation in the research at any time.

F. E-mail, Message Boards, and Forums

Email is not a secure communication mechanism and PIs and research staff must take into account the risks associated with contacting subjects via email. It is important to keep in mind that 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. Researchers are advised against including sensitive information in emails including the subject line. When collecting the subject's email address as part of the contact information, investigators should remind the subject of these considerations and risks.

Another risk is sending an email to the wrong address. Investigators should take reasonable steps to make sure the email is received by the correct person. In general, email should not be used to collect data. All outgoing emails should be from the hospital's server and contain instructions relating to whom to notify if received in error.

Caution should be taken when communicating with research subjects via message boards or other online forums that do not ensure privacy. The IRB encourages investigators to review the terms of use of any venue before utilizing it.

G. Electronic Data Storage

The Institutional Administrative Policy on Classification and Handling of Information requires that laptops and computers that contain research data must be password protected and encrypted. When appropriate, the individual data files should also be password protected. Personally identifiable information (PII) should be stored separately from the data. Research data containing PHI or any of the HIPAA identifiers may not be placed on any personal use devices including home computers, laptops, or tablets.

Investigators must include in the Cayuse IRB Initial application a description of how long the data will be kept electronically and any provisions for destruction of the data and/or identifiers. Copies of electronic data files may be kept for back-up and security purposes and thus not destroyed.

H. Data Transmission and Security

The Institution requires that any data containing any of the eighteen HIPAA identifiers or otherwise sensitive information collected from human subjects over computer networks be transmitted in encrypted format of at least 256 bit. This ensures data security during transmission from the subjects' computer to the Web. Researchers who are planning to collect and transmit PHI and/or sensitive data via the Internet are required to contact Information Technology to assess the internet security arrangements for the Internet site(s) the study seeks to use.