The following are suggestions from the American Association for Public Opinion Research concerning methods to protect confidentiality during online surveys:

http://www.aapor.org/default.asp?page=survey_methods/IRBS_faq

Electronic recruiting and data collection pose some additional challenges to human protections primarily in the area of confidentiality. The key challenges can be broken down into 4 areas:

RECRUITMENT: Computer- and internet-based procedures for advertising and recruiting potential study subjects (e.g., internet advertising, e-mail solicitation, banner ads) should follow the IRB guidelines for recruitment that apply to any traditional media, such as letters, telephone scripts, newspapers and bulletin boards. 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. Researchers should take steps to authenticate respondents. For example, investigators can provide each study subject (in person or by letter) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer- and internet- based data collection.

DATA COLLECTION: It is often recommended that any data collected from human subjects over computer networks be transmitted in encrypted format. This helps insure that any data intercepted during transmission cannot be decoded and that individual responses cannot be traced back to an individual respondent. In addition, if the content of the responses would pose risk to the respondents if the information were shared, it is recommended that the highest level of data encryption be used, within the limits of availability and feasibility. This may require that the study subjects be encouraged or required to use a specific type or version of browser software. It should also be noted that encryption standards vary from country to country and that there are legal restrictions regarding the export of certain encryption software outside the U.S.

SERVER ADMINISTRATION: It is recommended that for online data collection a professionally administered survey server be used or that a) The server is administered by a professionally trained person with expertise in computer and internet security, b) Access to the server is limited to key project personnel and is configured with firewalls to minimize the possibility of external access to the server data, c) There are frequent, regularly scheduled security audits of the server, and d) The server is subject to the periodic security scans.

DATA STORAGE/DISPOSAL: If a server is used for data storage, personal identifying information and IP addresses should be kept separate from the data, and data should be stored in encrypted format. Data backups should be stored in a safe location, such as a secure data room that is environmentally controlled and has limited access. Competent data destruction services should be used to ensure that no data can be recovered from obsolete or discarded electronic media. For projects that are minimal risk, if these data security safeguards cannot be put in place, then language in the consent information should be added indicating that complete confidentiality cannot be guaranteed and/or that encryption of responses is not provided.