CORNERSTONE BEHAVIORAL HEALTHCARE

TELEMEDICINE RISK MANAGEMENT POLICY

Purpose:

The purpose of this policy is to ensure that risk directly related to the use of telemedicine at CORNERSTONE is identified, analyzed and managed so that it can be minimized to an acceptable level in order to secure the protected health information (PHI) of the agency's clients and reduce the possibility of vulnerabilities, liabilities and/or sanctions affecting or impacting the agency. A related goal is to ensure that risk mitigation is done in a proper, cost-effective and efficient manner should mitigation ever become necessary.

Scope:

This policy applies to the use and application of telemedicine technology in the normal course of business at the agency. It does not apply to other electronic modes of communication such as email, FAX, or telephone.

Definition:

Telemedicine is a mode of delivering healthcare services by use of an interactive audio/video system using leased digital telephone lines or the Internet for data and voice transmission.

Brief Description of Telemedicine:

The telemedicine configuration is quite basic. It is a system that enables audio/video interaction between parties at two separate facilities over a leased digital data/voice line or over the Internet. At both ends of the telemedicine conference is a PC equipped with a webcam and integrated microphone. A proprietary program application is used to contact the other facility and to then enable the telemedicine session while protecting its content through data encryption. Once the point-to-point connection is made, the participants at both facilities can see each other on screen and hear one another as well. To further visualize the technical configuration, a videophone conference on a secure line between two participants would be somewhat parallel to telemedicine. The important point is that like the videophone, the telemedicine call is encrypted

including both the video and audio aspects of the call. HIPAA does not have any regulations for telemedicine (or videophone) that are any more stringent than for a traditional land-line phone call between two parties which is considered to be a secure communication. Any written materials recorded and/or printed during the course of a telemedicine session do become PHI and must be protected as such under the regulations.

Benefits:

Benefits of utilizing telemedicine in healthcare include improved access to healthcare; improved continuity of care; patient education; timely treatment; and, improved access to medical records and information.

Session Documentation Needed to Reduce Risk of Liability:

AHIMA recommends that the telemedical record contain at a minimum:

Date of the telemedicine session

Clinician's name

Informed consent (if a new client)

Notice to the client that telemedicine records are included under the agency's disclosure policy

Type of service performed

Diagnosis/impression

Recommendations for further treatment

Regulatory Environment:

HIPAA

According to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, §§ 261-264, covered entities (and their business associates) have an affirmative duty to identify and respond to any security incident, including an impermissible disclosure, that is known or suspected. At the front end is the requirement for employee training to ensure that employees can properly perform their functions within the organization. Should an impermissible disclosure occur, the affirmative duty includes recording the details of the incident and retaining that documentation for a period of six (6) years. The response must also include

invoking sanctions against any employees or other members of the entity's workforce who violate the internal policies and procedures regarding disclosures. In addition, covered entities have a mitigation obligation upon improper disclosure of PHI. They must, to the extent practical, do what they can to lessen the harmful effects of any security incident pertaining to improper disclosure.

Clients have a right to adequate notice regarding the uses and disclosures of their PHI when clients request a written accounting, including impermissible disclosures. The entity has 30 days to produce the requested accounting. Covered entities are exempted from reporting routine disclosures made in the ordinary course of business (i.e., those pertaining to treatment, operations, and payment). Covered entities are NOT required to notify individuals of every impermissible disclosure, although they are required to produce information about them if an accounting is requested by the client. Thus, the entity must place a report in the medical record whenever any such impermissible disclosure of PHI occurs and becomes known. Under common law an individual whose PHI has been compromised has the right to initiate a lawsuit for damages despite mitigation efforts.

The implication for telemedicine is that sanctions and mitigation would certainly apply to any documents recorded and/or printed during the telemedicine session which are not fully secured; however, it would be far less likely that employees could detect a breach of electronic security during a telemedicine session.

Under HIPAA's privacy rule, to safeguard PHI, HIPAA requires covered entities to have in place appropriate administrative, technical, and procedural measures. The requirement most applicable to telemedicine would be technical safeguards. An example would be firewall protection for keeping the telemedicine system itself secure.

HITECH Act (Subtitle D of the American Recovery and Reinvestment Act of 2009)

More recent regulations were issued concerning notification of breach of PHI in August 2009, implementing section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH Act), part of the ARRA of 2009. This requires HIPAA-covered entities (and business associates) to provide notification to the client following any breach of unsecured PHI. Unsecured PHI information is defined as information that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified in guidance by the Secretary of the U.S. Department of Health & Human Services. For purposes of telemedicine, an encrypted program application would cause health information being used or discussed during a telemedicine conference to be indecipherable to an outside third party during data transmission. Covered entities that have secured PHI by causing it to be unusable, unreadable or indecipherable are relieved from providing notifications following the breach of such information.

State of Maine

The only law in the Maine Revised Statutes relating to telemedicine is Title 24-A: Maine Insurance Code, Chapter 56-A: Health Plan Improvement Act. The sole purpose of this statute is to prohibit an insurance carrier offering a health plan in Maine from denying coverage on the basis that the treatment is provided through telemedicine if the health care service would be covered were it provided through in-person consultation between the covered person and a health care provider. The statute does not outline any requirements for the security of protected health information while telemedicine is being utilized.

State Licensing standards for securing PHI would only be relevant if they were to be more stringent than federal HIPAA standards, which are, in fact, not the case. Therefore, HIPAA and ARRA are preemptive.

Accreditors:

Because CORNERSTONE is not accredited by JCAHO, CARF, COA, or other accreditor, there are no additional standards to be met for handling telemedicine within the agency.

Identification of Potential Risk:

Primary risk associated with the use of Skype for Telemedicine is that the sessions between the provider and the client could be intercepted at a remote node due to Skype being pier to pier. This risk is mitigated by the fact that the Skype software uses 256 bit encryption to secure communication even as it travels over a remote node and would therefore be undecipherable by a third part without significant effort (2 to the 70^{th} computations minimum). Skype also uses a 1024 bit AES encryption to exchange pass codes when establishing communication with a remote site to ensure that the proper individual is receiving the information.

Plan

1. In the event that it has become apparent that Skype has been compromised as secure software, all sessions will immediately be discontinued with the use of that software.
2. Any clients who have outstanding appointments for Telemedicine will be rescheduled in an orderly fashion to be seen by the provider in person or offered another viable solution as soon as possible.
3. In the event of a known breach of encrypted information during a telemedicine session, no notification must be made to the client, as the HITECH Act in the ARRA does not require notification for breach of secured information. The breach, however, will be

documented in the medical record to be part of any future accounting requested by the client as required by HIPAA

Additional Reference Materials:

Appendix A : Statement of Security from the White Pages for Skype 3.0 for Network Administrators.

Appendix B: American Recovery and Reinvestment Act of 2009/Division A/Title XIII/ Subtitle D.

Donna M. Rubell, LCPC

Executive Director/ Date 12-23-10

Revised:12/13/10