Alliance
BEHAVIORAL HEALTHCARE

Developing a Policy and Procedure for the Protection of Privacy and the Secure Storage of Records

HIPAA Compliance

- HIPAA Security Rule requires covered entities (ex. mental health practitioners) to perform risk analysis as part of their security management processes
- Providers must ensure confidentiality, availability and integrity of the record
- Provider must determine which security measures are reasonable and appropriate for their practice

HIPAA Compliance

- Risk analysis affects the implementation of all of the safeguards contained in the Security Rule
- This training designed to help you think about what you need to do to protect your practice
  - Not all items discussed in the training will pertain to what you do but can be used as a resource to help you think about HIPAA compliance

Risk Assessment

- Before developing a policy and periodically thereafter, conduct risk assessments and identify resulting safeguards
  - Evaluate likelihood and impact of potential risks
  - Implement appropriate security measures to address the risks identified in the risk analysis
  - Document the chosen security measures and where required, the rationale for adopting those measures
  - Maintain continuous, reasonable and appropriate security protections

Risk to be Considered

- Risks that must considered in policy and procedure
  - Instability over time due to deterioration of material
  - Improper storage (temperature, humidity, dust, light)
  - Overuse
  - Human and natural disasters
  - Infrastructure failure (plumbing, electrical, climate control)

(reference APSM 45-2 Records Management and Documentation Manual)

Risk to be Considered

- Risks that must considered in policy and procedure
  - Inadequate hardware maintenance (locked cabinets, locks on doors, etc.)
  - Malfunction of hardware
  - Human error and improper handling

(reference APSM 45-2 Records Management and Documentation Manual)

What Your Risk P&P Must Address

- The safeguarding of service records against loss, tampering, defacement, use or disclosure by unauthorized persons
- Making service records readily accessible to authorized users at all times

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Protecting confidential information stored in portable computers
  - Loaning and using portable computers
  - Purging confidential data from computers
  - Encryption of PHI (ex: emails)
- Securing information being faxed
  - At a minimum, procedures required if confidential information is to be faxed, including verifying fax number with receiving party and checking to ensure receipt of fax

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Safeguarding email (encryption, password protection)
  - If email is used to communicate confidential information, a policy regarding how the confidential information will be secured and protected
  - Unless provider agency has capability to encrypt email, emailing of confidential information should be the least preferred method of transmitting information and be used only when the information is password-protected as outlined below

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Using Electronic Medical Records (authorized users, signatures, errors) – at minimum:
  - Policy defining the classifications of information (data sets) to which different users may have access
    - Will see this more for group practices or additional administrative staff who have access to files

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Using Electronic Medical Records (authorized users, signatures, errors) – at minimum:
  - Policy specifying that only authorized users have access to service recipient information, based on minimum necessary principles defined in by HIPAA
    - Measures such as passwords and audit trails to help ensure that only identified users have access to the minimum amount of service recipient information necessary to complete their job function

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Protecting, disseminating or disclosing confidential information (Releases of Information, HIV, SA, Exceptions to Prior Authorization)
- Transporting records securely (locked compartment, lost or stolen, why transport is necessary, who can transport)
- Storing, maintaining, and destroying records consistent with the principles of privacy and security

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Service records shall only be transported by individuals designated by the agency
  - When original service records removed from facility premises, efforts shall be made to ensure that the records are packaged safely and securely
  - When transported by motor vehicle, service records shall be secured in a locked compartment (e.g. locked car, locked trunk, or locked briefcase)

(reference APSM 45-2 chapters 2-7 to 2-10)

What Your Risk P&P Must Address

- Service records shall only be transported by individuals designated by the agency
  - P&Ps on transporting records shall be developed by the provider agency to include detailed instructions for what the individual must do in the event that confidential information is lost or stolen
  - Should facility determine it is not feasible or practical to copy the service record or portions thereof, service records may be securely transported to a local health care provider, provided the record remains in the custody of a delegated employee

(reference APSM 45-2 chapters 2-7 to 2-10)

Storing and Maintaining Service Records

- Records should be protected from theft, unapproved use, and damage or destruction
- Safeguards should cover the possibility of harm by fire, water and natural disasters
- Records must be destroyed in a manner that safeguards confidentiality and privacy
- Though service records should be safeguarded carefully, they also must be available to be used

(reference APSM 45-2 chapters 2-9 to 2-10)

Electronic Records

- Electronic Records Agencies utilizing an electronic service record must develop procedures staff required to follow when corrections necessary in the service record
  - Corrections made by the individual who recorded the entry (APSM 45-2 Service Notes and Service Grids Chapter January 1, 2008/April 1, 2009 9-4)
  - Corrections electronically signed and dated
  - Original text not deleted
  - Explanation of type of documentation error included whenever the reason for correction is unclear

(reference APSM 45-2 chapters 9-3 to 9-4)

Additional Resources

- NC Guidelines for Managing Public Records Produced by Information Technology Systems
  - Developed by Government Records Branch, Archives and Records Section, NC Division of Historical Resources
  - Guidelines for development and monitoring of electronic records
  - Entities maintaining electronic records should conduct a self-warranty process and develop an electronic records policy
  - www.ah.dcr.state.nc.us/records/e_records/default.htm

Additional Resources

- Centers for Medicare and Medicaid Services (CMS)
  - Federal agency that administers Medicare, Medicaid, and State Children's Health Insurance Program
  - HIPAA Security Information Series
    - Introduction to organizational security issues and guidance
    - www.hhs.gov/hipaa/for-professionals/security/guidance/

Responding to a Breach of PHI

- Investigate the incident to determine if an actual breach has occurred
  - Document findings
  - Notify affected consumers
  - Notifying DHHS Office of Civil Rights and the Attorney General's office
  - Notify Alliance if you have a Business Associate Agreement
    - Breach in confidentiality considered a Level I incident if you provide services (enhanced) in addition to outpatient

Summary

- Proper handling of medical records and other protected health information facilitated by a process including these provider activities:
  - Assess current security, risks and gaps
  - Develop an implementation plan
  - Implement solutions
  - Document solutions
  - Reassess periodically

Additional Resources

- To ensure compliance it is beneficial to review HIPAA Privacy and Security Rules regarding HIPAA protections and guidelines that practitioners are required to follow
  - www.hhs.gov/hipaa/index.html
  - http://hipaa.dhhs.state.nc.us/index.html
  - www.hipaa.org/
  - www.socialworkers.org/hipaa/primer0806.pdf
  - www.ncdhhs.gov/providers/provider-info/mental-health/records-management