I HAVE ALL THESE RECORDS. NOW WHAT?
Agenda

- Public Records Law
- When Provider Agencies Merge or Go Out of Business
- Record Retention
- Record Destruction
- Disaster Plan
- Electronic Records
- Electronic Signatures
- HIPAA
Public Records Law
Within the public DMH/DD/SAS system, private provider consumer service records and records supporting the expenditure of state and federal funds which are created by private providers are considered public records because they relate to the transaction of public business by LMEs, the Division of Medical Assistance, and DMH/DD/SAS.
What is included?

- Includes e-mail, documents (including drafts), texts, papers, electronic processing records, pictures, video tapes etc. regardless of physical form or characteristics, made OR received in connection with the transaction of public business by any agency of NC or its subdivisions.
What is excluded?

- Attorney-Client Communications
- Trial Preparation materials
- Records deemed confidential under NCGS 122C
- Trade and Corporate Secrets
- Blueprints
- Certain criminal investigation/intelligence records
Procedural Requirements for Disclosing Public Records

1. Which Agency Must Provide Access?
2. Can the Custodian of the Files Ask Why the Records are Being Sought?
3. When Should Access Be Provided?
4. Can I Charge a Fee for Copies?
5. Can I Require the Request Be In Writing?
6. What Format Must Copies Be Provided?
Basic Rules around Public Records Law

- Anyone may inspect and receive copies of public records
- Must cite specific statute or federal law when access is restricted or denied
- Cannot ask what it will be used for
- Requestor can ask for a specified format
Agency Mergers and Closures
Agency Mergers

- Agency that created the record is still responsible for maintaining records for duration of retention schedule, including custody. (APSM 45-2 Chapter 1-3)

- Service records have two distinct components: the clinical record and the financial record. The financial record includes billing and reimbursement information. Reimbursement information includes any administrative records that document that staff held proper credentials to provide the service (personnel records).
• Have consumers sign a release of information form.
• Make copies of the record to send to the new treating provider.
• Develop a retention and disposition plan outlining how the records are stored, who will be the designated records custodian and how will the LME/MCOs be informed of what the process is and where the records are located.
Agency Closures in NC

If your agency ceases to provide services in the State of NC:

Complete the Record Storage log found on our website

Providers to Medicaid consumers-
• Submit the original medical records for all consumers served on and after 2-1-2013 to Alliance.

Providers to IPRS and Medicaid consumers –
• All IPRS consumer records and any Medicaid consumers discharged before 2-1-2013 are required to store and maintain the records until they have met their retention. This includes processing release of information as requested. Once logged, the log shall be submitted to Alliance.

Failure to maintain records per the retention schedule can result in reporting to DMA Program Integrity, Office of Civil Rights and your licensing board.
Agency Closures cont.

- If you have an electronic record, you will need to print out the records to submit to Alliance.

- If you serve consumers that are in multiple catchment areas, notify each LME/MCO. Records shall be turned over to each LME/MCO based on the location where the consumer was served.
Record Retention and Destruction
**APSM 10-5** - Records Retention and Disposition Schedule for DMH/DD/SAS Provider Agency

- Must be Acknowledged by Agency Director and Chairman of Agency Board
- Once approved, mail in to Cultural Resources
- This schedule is the way Department of Cultural Resources gives you consent to destroy records

**Grant schedule** - published 2 times a year from Office of the Controller - need to follow due to not knowing where money is received from.

- Retention is generally 10 years
HIPAA - 45 CFR 164.316(b)(2). 6 years from date of creation or date it last was in effect, whichever is later. Does not specify medical record retention requirements, it does require that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other protected health information (PHI) for whatever period such information is maintained by a covered entity, including through disposal.

Medicaid - Six years per February and June 2013 Medicaid bulletins.

Electronic Discovery – Title V-Federal Rules of Civil Procedure

Required to follow the more stringent rule.

No record involved in a pending audit, legal or other official action may be destroyed before that audit or action is resolved.
Retention Timeframes

Service record-components-medical and financial

- Adult Service Records- 11 years from DOLS
- Minor-age of majority (18) + 12 years
- DWI- 15 years
- Personnel- Official file 30 years
- Finance- 6 years but 10 years per grant schedule
- Permanent records- forever and must have a preservation copy. Can either be paper or microfilm.
- E-mails- depends on the subject of the e-mail
Before you Destroy

Before any records are destroyed, the following has to occur (APSM 10-5):

- Ensure the records have met their retention
- Log the information being destroyed (sample log is provided on DMH website)
- Ensure your Director and Board Chair has approved the retention schedule
- Inform your governing body of the planned destruction
- If using a company to destroy your document, make sure you have a signed contract and a Business Associate Agreement in place.

Serving Durham, Wake, Cumberland and Johnston Counties
Destroying Confidential Information

**Paper:**  
Shred (≤3/8")  
Acid vats to reduce to pulp  
Incinerate  
Sold as waste paper, provided that the purchaser agrees in writing that the documents or materials will not be resold without pulverizing or shredding the documents so that the information contained within cannot be practically read or reconstructed.

**Back-up tapes and computer hard drives:**  
Overwrite  
Degauss  
Physically destroy

**Magnetic media:**  
Overwrite  
Expose to a magnetic field
Destroying Confidential Information cont.

Remember to include the following:

- Copiers
- Fax Machines
- Typewriters
- Shred bins
- USB Drives
- Mobile Devices

Don’t throw away PHI in a trash can.
Record Destruction

- Destruction logs shall include:
  - Date of Destruction
  - Method of Destruction
  - Description of the Disposed Records
  - Inclusive dates
  - Statement the records were destroyed in the normal course of business
  - Signatures of individuals supervising and witnessing destruction
If destruction services are outsourced to a business associate, be sure the contract includes the following elements:

- The method of destruction or disposal
- Time that will elapse between acquisition and disposal
- Safeguards against breaches
- Indemnification for the organization or provide for the loss due to unauthorized disclosure
- Request the BA to maintain liability insurance in specified amounts at all times
Legal Risks

- Records that are not destroyed according to their retention schedule are subject to discovery during litigation, investigations, and Freedom of Information Act (FOIA) requests.

If you have it, you must produce it.

- Shredding/Destroying records before they have met retention can result in monetary fines, contempt charges, criminal and civil penalties, and loss of licensure.
Abandonment of Records

DHHS has issued a statement that any LME/MCO that becomes aware of a provider that has abandoned records (medical, financial and/or personnel) shall be reported immediately to DMA-PI. As this is also a violation of confidentiality, a report will also be made to OCR and your licensing board.
Disaster Plan for Records

How will your information, paper and electronic, be protected against:

- Loss
- Theft
- Destruction
- Unauthorized access
- Natural Disasters

It is recommended that a risk assessment be performed in order to assess the vulnerability of the environment in which all records are stored.
Electronic Records
Records Duplicated by Electronic Means

Before you begin:
- Make sure the records are not considered permanent records
- Complete the Self Warranty process
- Electronic Records Policy-approved by DCR
- Complete the Request to Destroy Records Duplicated by Electronic Means

This information can be found on the Department of Cultural Resources website at


Serving Durham, Wake, Cumberland and Johnston Counties
Computerized Records

- A covered entity that creates, accepts, modifies and transmits ePHI must be able to show that its computer system is reliable and that its records are legible, accurate, confidential and trustworthy.
- Documentation is key as are proper and continuous training of personnel, development and implementation of adequate policies and procedures and maintenance of computer system hardware and software.
- A covered entity must be able to demonstrate how ePHI was created and maintained by the covered entity including the sources of information on which the ePHI was based.
- The covered entity must also be able to demonstrate its procedures for retrieving information and the controls and checks it has in place to ensure that the record is accurate and reliable.
To ensure that 1) the ePHI created modified and transmitted by the covered entity is accurate and 2) that the covered entity can authenticate its computerized records, the following shall be implemented:

Entries and Corrections-
- Errors shall be corrected appropriately, by the person that created the error and in a uniform manner according to the covered entity's policy.

System Monitoring-
- The covered entity should have in place software programs that automatically records the time and date of entries including modifications as well as the identity of the person making the entry or modifying the record and even who has viewed the record.

System Testing-
- The computer system should periodically be tested and the hardware properly maintained and updated as needed.

See AHIMA eHIM Workgroup on Maintaining the Legal EHR Update
Record Maintenance-
- The same information should be preserved for both the original entry and later correction to show that the change was not part of a cover up.

Security Features-
- Administrative, physical and technical safeguards including password protection encryption and other security measures.
- Ability to create an exact duplicate.

Education and Training-
- Personnel who access, create and modify ePHI are required to be trained in proper data entry, access and security protocol and educated about system vulnerabilities and threats.

Remember-the medical record, whether paper or electronic, is a legal document.
The laws that apply to traditional paper records also applies to electronic records including public records and retention laws.

Maintain the associated metadata (APSM 10-5, Standard 3). Each electronic form uploaded or created in the digital signature software will have metadata that describes, explains, or locates the form. Metadata can be generated by the system, software, or the user. The system should be able to create a summary report that includes a certificate of completion, record tracking, IP addresses, time stamps, and other important data that validates the document.
Electronic Communication with Alliance

Alliance requires that all communications involving PHI be encrypted. If Alliance sends you an encrypted e-mail, any communication within that e-mail is encrypted.

Visit the Provider section of our website on how to generate an encrypted e-mail.
Electronic Signatures

- NC General Statutes 90-412 Electronic Medical Records establishes the use of electronic medical records and esignatures in North Carolina.

- "Electronic signature" as defined by UETA: “an electronic sound, symbol, or process attached to, or logically associated with, a record and executed or adopted by a person with the intent to sign the record.”

Use of a font in Word does not constitute an electronic signature.
§ NCGS 66-58.5. Validity of electronic signatures.

- (a) An electronic signature contained in a transaction between a person and a public agency, shall have the same force and effect as a manual signature provided all of the following requirements are met:
  - (1) The public agency involved in the transaction requests or requires the use of electronic signatures.
  - (2) The electronic signature contained in the transaction embodies all of the following attributes:
    - a. It is unique to the person using it;
    - b. It is capable of certification;
    - c. It is under sole control of the person using it;
    - d. It is linked to data in such a manner that if the data are changed, the electronic signature is invalidated; and
    - e. It conforms to rules adopted by the Secretary pursuant to this Article.

- (b) A transaction undertaken between a person and a public agency, or between public agencies, is not unenforceable, nor is it inadmissible into evidence, on the sole ground that the transaction is evidenced by an electronic record or that it has been signed with an electronic signature.
Electronic Signatures cont.

- Healthcare providers may permit authorized individuals to authenticate orders and other medical records by electronic or digital signature in lieu of a signature in ink.
- The individual who made or authorized the entry shall authenticate medical record entries in this fashion.
- Authentication is defined as the process of verifying that a document or record is genuine or original. In the case of electronic documents, it is the process of confirming a user’s identity.
Electronic Signatures cont.

- Authentication must be accomplished by signature, initials, computer entry or code or other methods not inconsistent with the laws, rules and regulations or any other applicable jurisdictions.
- Once a document has been signed, it cannot be deleted or altered in any way.
- If an error is discovered on a signed document, an addendum to the document shall be created.
- Your login and password is how you are identified most of the time when an electronic signature is used. Never share your login or password with anyone.
Electronic Signatures cont.

- Things to remember:
  - Have policies and procedures been developed and are they being followed?
  - Metadata is required to be maintained. It provides answers to questions like “what is it”, “where did it come from,” and “who created it.”
  - It is a violation to ask consumers to sign blank documents.
  - Do not save consumer signatures to apply to other documents. This is considered fraud.
HIPAA
Who Must Comply With HIPAA?

- There are two basic elements for determining who is required to comply with HIPAA. First, a person or entity must be a health care provider, health plan, or health care clearinghouse to be covered by HIPAA. Second, a person or entity must electronically transmit health information for payment or administrative purposes.
Penalties for failing to Comply- Civil Sanctions

Failure to comply with general HIPAA requirements and standards is punishable as follows:

- Maximum of $100 per violation per person or organization
- Not to exceed $25,000 in a calendar year for multiple violations of the same requirement.
- Civil sanctions do not apply to knowing disclosures of PHI
- 42USC 1320d-5
HIPAA imposes criminal penalties for wrongfully obtaining individually identifiable health information or for improperly disclosing individually identifiable health information to another person. Criminal penalties will be levied for:

- Knowingly using or causing to be used a unique health identifier for improper purposes
- Obtaining individually identifiable health information relating to an individual or
- Disclosing individually identifiable health information to another person

Criminal penalties include:

- For the offense of knowingly obtaining protected health information-- up to a $50,000 fine or imprisonment for up to one year or both
- For the offense of obtaining protected health information through false pretenses-- up to a $100,000 fine or imprisonment for up to 5 years or both.
- For the offense of intending to sell protected health information: up to a $250,000 fine, imprisonment for up to 10 years or both.

An example of this offense is when an individual obtains protected health information and then attempts to sell or sells the information to a third party for money or personal gain.
HIPAA Audit Program Protocol

- **Privacy-81 requirements** - covers 1) Notice of Privacy Practices for PHI, 2) Rights to Request Privacy Protection for PHI, 3) Access of Individuals to PHI, 4) Administrative Requirements, 5) Uses and Disclosures of PHI, 6) Amendment of PHI, 7) Accounting of Disclosures

- **Security-78 requirements** - covers administrative, physical, and technical safeguards

- **Breach- 10 requirements** - covers Breach Notification Rule
1. Notice of Privacy Practices
2. Minimum Necessary Disclosures
3. Accounting of Disclosures
4. Access to PHI
5. Amendment of PHI
6. Alternative Contact Requests
7. Privacy Related Complaints
Changes to HIPAA enacted by the Omnibus Final Rule

- All healthcare business associates and subcontractors are now covered under HIPAA Privacy Rule.
- Definition of BA expanded- includes subcontractors that create, receive, maintain, or transmit PHI on behalf of another BA. Also includes:
  - Health information organizations
  - E-prescribing gateways
  - A person that provides data transmission services for PHI exchange on behalf of a CE and requires access to such information on a routine basis
- BA now liable to CE for the activities of the subcontractor.
- The Security Rule requires that a Business Associate (“BA”) implement three types of safeguards: 1) administrative, 2) physical, and 3) technical
Breach Under HITECH

- Breach now defined as “the acquisition, access, use, or disclosure of PHI in a manner which compromises the security or privacy of the PHI.

- Burden on the CE, BA or subcontractor to demonstrate low probability that the PHI has been compromised, otherwise breach notification is required.

- Risk Assessment is required to determine the level of compromise unless the consumer is notified.

- Annual Reporting
  - Required to report all breaches to OCR within 60 calendar days of the new year (due by end of February).
  - Ensure you have a tracking system
Resources

- OCR HIPAA Audit link- [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html)
- Division of MH/SA/DD- [http://www.ncdhhs.gov/mhddssas/providers/recordsmanagement/index.htm](http://www.ncdhhs.gov/mhddssas/providers/recordsmanagement/index.htm)