Confidentiality Practices in CCS

Jessica Beauchamp LCSW, SAS
Off The Couch Counseling and Consultation
White Pine Consulting

1

Contents:

- Introduction
- Overview of statutes/rules
- Confidentiality in specific scenarios
  - Paper and electronic documents
    - Transporting documents
  - Technology
    - Laptop/home computers
    - Wireless technology
    - E-mail and fax
  - Conversations
- Disposing of Records
- Reporting recommendations
- Resources

2

Introduction

- You are part of professional community
- Access to client information carries with it responsibility
- Confidentiality is a cornerstone, protect it
- If you are unsure about sharing client information, defer to the team

3

Overview of The Statutes/Rules

4

WI Chapter 51.30: Records

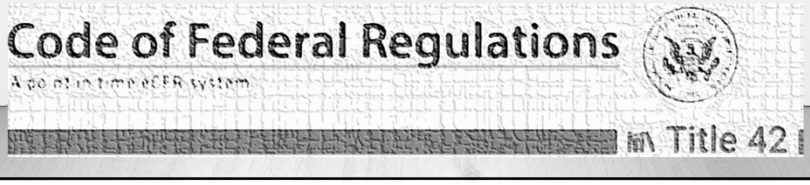
- *Treatment records* include all records that are created in the course of providing services to individuals for mental illness, developmental disabilities, alcoholism, or drug dependence and that are maintained by the department; by county departments and their staffs; by treatment facilities; or by psychologists or licensed mental health professionals who are not affiliated with a county department or treatment facility.
- An *informed consent* for disclosure of information from court or treatment records to an individual, agency, or organization must be in writing.

All treatment records shall remain confidential and are privileged to the individual

5

42 CFR Part 2: Confidentiality of Substance Use Disorder Patient Records

- *Patient identifying information* means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient can be determined with reasonable accuracy either directly or by reference to other information.
- *Records* means any information, whether recorded or not, created by, received, or acquired relating to a patient. For the purpose of the regulations in this part, records include both paper and electronic records.
- *2.16 Security for records.* The holder of patient identifying information must have in place policies and procedures to reasonably protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information.



6

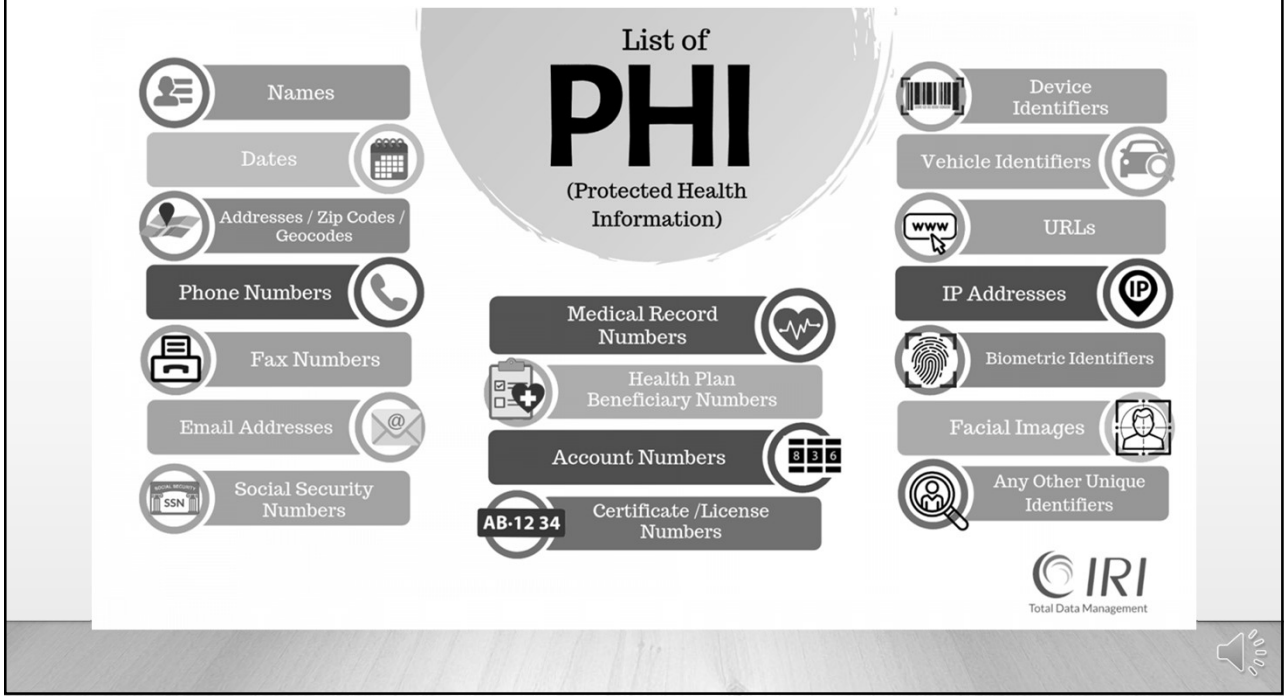
HIPAA:
The Health Insurance Portability and Accountability Act

- Addresses how healthcare organizations are required to treat patient records when an individual is being treated for mental health conditions.
- "Protected health information (PHI) is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations."
- "PHI relates to physical records, while ePHI is any PHI that is created, stored, transmitted, or received electronically."
- "PHI is only considered PHI when an individual could be identified from the information. If all identifiers are stripped from health data, it ceases to be protected health information and the HIPAA Privacy Rule's restrictions on uses and disclosures no longer apply."

HIPAA
Health Insurance Portability & Accountability Act

www.hipaajournal.com

7



8

Confidentiality in specific scenarios

9

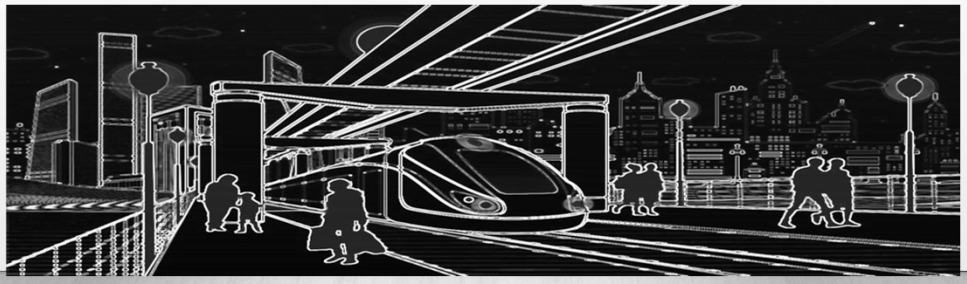
Paper and Electronic Documents

- Documents containing personal information may be either in paper or electronic format
- All paper and electronic data is confidential
- Documents containing personal information should be secured
- Obligation is on you to actively ensure security of paper and electronic documents

10

Transporting Documents

- Secure in folders, carried in a locked briefcase or sealed box
- Should not be opened or viewed while traveling
- Kept under the constant control of you while in transit



11

Laptop/Home Computers

- Access to laptop/home computers should be password-controlled
- Data stored on the hard drive should be encrypted
- Anti-virus software and personal firewalls should be installed
- Ensure that the screen cannot be seen by anyone else
- Should be logged off and shut down when not in use
- Do not share a laptop that is used for work purposes with other individuals
- Video platforms to communicate with clients must ensure that communications are secure

12

Wireless Technology

- Devices should be password-controlled
- Any stored data should be encrypted
- Ensure that the display panel cannot be seen by anyone else
- Avoid using cell phones to discuss client information outside of a secure setting
- Avoid disclosing any personal health information in text format
- Maintain constant control of wireless devices
- Do not share wireless devices that are used for work purposes with other individuals
- Avoid using a public internet connection or free Wi-Fi service

13

E-mail/fax

1. You either need to be 100% sure that ONLY your recipient gets the email/fax, or

2. You need to get permission to send unsecure email/fax AND tell them about the risks

- **When we send you an email, or you send us an email, the information that is sent is not encrypted. This means a third party may be able to access the information and read it since it is transmitted over the Internet. In addition, once the email is received by you, someone may be able to access your email account and read it.**
- Email is a very popular and convenient way to communicate for a lot of people, so in their latest modification to the HIPAA act, the federal government provided guidance on email and HIPAA
- The information is available in a pdf (page 5634) on the U.S. Department of Health and Human Services website - http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- The guidelines state that if a patient has been made aware of the risks of unencrypted email, and that same patient provides consent to receive health information via email, then a health entity may send that patient personal medical information via unencrypted email

OPTION 1 – **ALLOW** UNENCRYPTED EMAIL
I understand the risks of unencrypted email and do hereby give permission to the Austin Med Clinic to send me personal health information via unencrypted email

Signature (parent or guardian if patient is a minor)	Date	Printed name	Please print email address

OPTION 2 – **DO NOT ALLOW** UNENCRYPTED EMAIL
I do not wish to receive personal health information via email

14

Conversations

1. WHAT? is being discussed
2. WHERE? the discussion takes place
3. WHO? is listening
4. WHY? the discussion took place

15

Confidential Information Sharing Do's

1. Do treat all information regarding clients with respect
2. Do share information regarding client's academic, behavioral, or family situation only with team members
3. Do discuss confidential client information in settings that are private enough that confidential information is not inadvertently disclosed
4. When in doubt as to whether to disclose information, do refrain from sharing the information and ask the service facilitator/care coordinator
5. Do store confidential records/documentation in a secure location

16

Confidential Information Sharing Don'ts

1. Do not discuss confidential information in public places (grocery store, parking lot, etc.) where information may be inadvertently disclosed
2. Do not discuss academic, behavioral, or family situations with anyone who does not have a reason to know the information
3. Do not leave confidential records/documents where those without legitimate purpose may see it

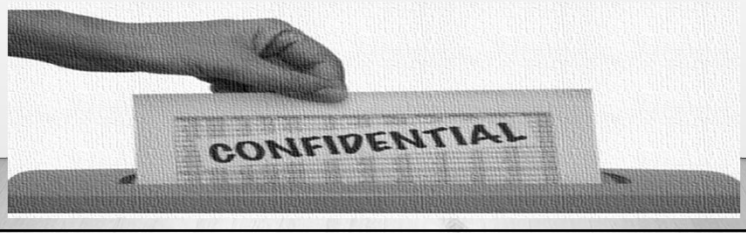
17

Disposing of Records

1. Shred or burn them, or contract with a professional disposal firm
2. Do not dispose of documents in areas that are accessible by the public or other unauthorized persons
3. The only safe means of disposing of computer-based information requires physically removing and destroying the hard drive

42 CFR Part 2.19 Disposition of Records

"Remove patient identifying information from its records or destroy its records, including sanitizing any associated hard copy or electronic media, to render the patient identifying information non-retrievable in a manner consistent with the policies and procedures"



18

Reporting Recommendations

The loss or theft of client information should be reported immediately to the Department you are contracted with.

19

Would patient information such as "Mr. Brown from New York" be considered PHI?

Although there could be thousands of Mr. Browns in New York, there is likely no more than a handful of Mr. Jakowskis in Crivitz, WI. As it would be impractical for HIPAA to stipulate there has to be fewer than so many Mr. Xs in a population of Y before the two identifiers are considered to be PHI, all combinations of identifiers are considered PHI under HIPAA – even "Mr. Brown from New York".

Are email addresses that don´t reveal a person´s name considered identifiers for PHI purposes?

It is simple to find out who an email address such as "anonymous@xyz.com" belongs to by doing a little research on social media or using a reverse email lookup tool on the Internet. Even if social media or a reverse lookup tool does not give you the individual´s name, you will still be able to find enough information about the individual for that information – with the email address – to be considered PHI.

When the teacher was asked if her CCS documents are secured, she replied, "Yes, I keep them in my desk drawer, and when I leave the classroom, I lock the classroom door." Is she correct, are they secured?

No. Her files are not secure because anyone with a key to her room has access. It is better to have a file cabinet or desk with a lock.

A social studies teacher and a special education teacher were sitting in the teachers' lounge discussing a child they both were on the CCS team for. They called the child by name and talked about his behavior problems, his family situation, and his disability. Were the teachers violating confidentiality?

If the teachers were discussing the child in private (no other teachers in the lounge or not within earshot of others) and they had a legitimate need to discuss the child's information, they were probably not violating the child's confidentiality, but they should monitor what they say if others come in.

20

Resources

42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2

WI Chapter 51.30: Records
https://docs.legis.wisconsin.gov/statutes/statutes/51/30

HIPAA Journal
www.hipaajournal.com

21