Confidentiality and HIPAA

DBHDD Behavioral Health Symposium
Presented by Elizabeth Bentley Watson
DBHDD Attorney
and HIPAA Privacy Officer
betty.bentley.watson@dbhdd.ga.gov
October 2016

Disclaimer

- This presentation does not constitute legal advice.
- Providers should seek their own legal advice from their own attorneys on these subjects.
- DBHDD Policies and forms are available for your review at DBHDD PolicyStat:

https://gadbhdd.policystat.com/

- You are welcome to copy DBHDD policies, but DBHDD does not guarantee that they will ensure your compliance with all laws applicable to you or your circumstances!

Confidentiality Count$!

HIPAA federal civil monetary penalties against healthcare providers by the U.S. Department of Health and Human Services have ranged from:

$35,000

to

$4.8 Million

Note that "willful neglect" in a breach will bring a civil money penalty.

See handout on "United States Health and Human Services 'Resolution Agreements' Regarding HIPAA Violations."

Topics for Presentation

- Various Confidentiality Laws and HIPAA
- Privileged communications
- HIPAA Basics
- Electronic PHI
- Reminders for risk prevention
- Sanctions
- Georgia Health Information Network (GaHIN)

See also: Citations in the slides and on handouts.

Why Confidentiality?

- To prevent stigma
  - Potential negative impacts to the individual in employment, relationships, economic status, even possible criminal charges for drug addiction information.
- Keep trust in treatment relationships
- Recovery!
- It's the law
- Other reasons?

Confidentiality and HIPAA

Confidential:

The property that data or information is **private** and is not made available or disclosed to persons who are not **authorized** to access such data or information.

HIPAA-speak: "Protected Health Information (**PHI**)"

45 C.F.R. § 164.304

DBHDD Policy 23-100 "Confidentiality and HIPAA"

Confidentiality and HIPAA

ALL information about individuals is confidential!!
In every form:

- Clinical and billing records
- Letters, documents
- Conversations
- E-mails
- Text messages
- Voice mail messages

45 C.F.R. § 160.103

Confidentiality and HIPAA

Disclosure – The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Disclosure includes:

- affirmative verification of another person's communication.
- communication of any information on an identified individual.

45 C.F.R. § 160.103

Disclosures of Confidential PHI

After a disclosure is made:

The information is *still confidential!*

A disclosure to Ms. Q that is valid under the law does not authorize disclosure to Mr. B, C, or D.

O.C.G.A. §§ 37-3-166(c), 37-4-125(c), 37-7-166(c)

"It's not just HIPAA!!"

Which law is the least strict on confidentiality??

1. Federal Law - Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2.
2. State laws - confidentiality for mental illness, developmental disabilities and addictive disease.
3. *Health Insurance Portability and Accountability Act of 1996 (HIPAA).*

Federal Regulations: Confidentiality of Alcohol and Drug Abuse Patient Records

Records and information *identifying an individual* as having an alcohol or drug abuse diagnosis are confidential, and cannot be disclosed without:

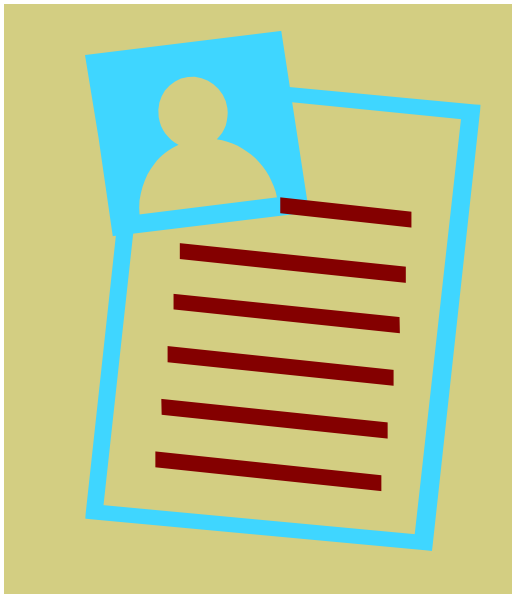
- Written consent of the individual (or a person authorized to give consent), OR
- Specific authority in the regulations.
- Alcohol and drug abuse records CANNOT be produced in response to a subpoena!

42 C.F.R. Part 2

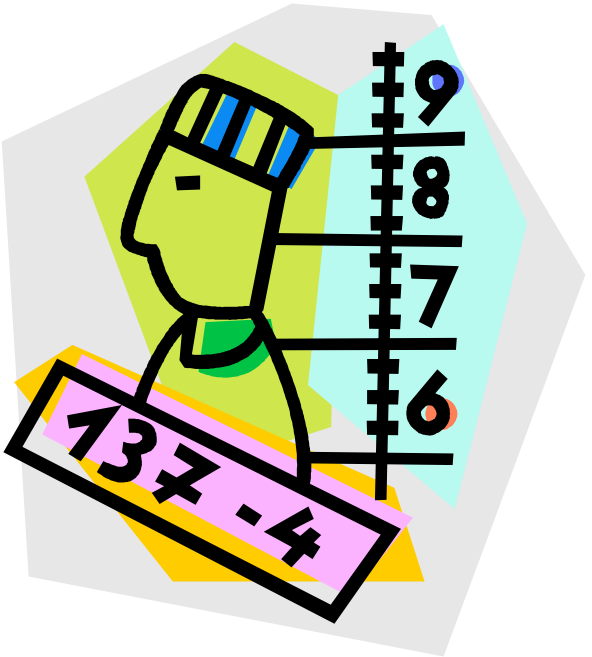
Federal Regulations: Confidentiality of Alcohol and Drug Abuse Patient Records

"Identifying an Individual":

Alcohol and drug information…



may incriminate!



Federal Regulations: Confidentiality of Alcohol and Drug Abuse Patient Records

Alcohol and drug abuse records which are produced on the individual's authorization must bear **notice** to the recipient concerning restrictions on further use or disclosure by the recipient.

Federal Regulations: Confidentiality of Alcohol and Drug Abuse Patient Records

CONFIDENTIAL AND PRIVILEGED

This information has been disclosed to you from records protected by Federal confidentiality rules (42 C.F.R. Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

42 C.F.R. § 2.32 (emphasis added)

Georgia Laws: Mental Health and Developmental Disabilities Records

Confidentiality of mental health and developmental disabilities information:

All information about individuals, whether oral or written and regardless of the form or location in which it is maintained, is confidential and may be disclosed only:

- When the individual (or another person authorized to do so) gives written consent, OR
- When the law specifically authorizes disclosure.

O.C.G. A. §§ 37-3-166 and 37-4-125
DBHDD Policy 23-100, "Confidentiality and HIPAA"

Georgia Laws: Mental Health and Developmental Disabilities Records

Georgia law authorizes disclosures of mental health and developmental disability records:

- To physicians or psychologists for continuity of care.
- To clinicians in a bona fide medical emergency.
- To the guardian or health care agent of an individual, or parent or legal custodian of a minor.
- To the individual's attorney, if authorized, AND if requested, at a hearing held under the Mental Health Code.
- For records of a deceased individual, to the administrator or executor of the estate AND in response to a subpoena by the coroner or medical examiner, ***EXCEPT*** for privileged information.

Georgia Laws: Mental Health and Developmental Disabilities Records

Lawful disclosures, mental health and developmental disabilities records, *continued*:

- For crimes alleged to occur on program premises, law enforcement may obtain circumstances of the incident and may be told whether an accused individual was hospitalized, and the individual's name, address and last known whereabouts.
- For crimes elsewhere, law enforcement may be told whether an individual has been hospitalized, and obtain the last known address of the individual.
- Upon request and upon authorization by the individual, notice of discharge of an adult involuntary individual may be given to the sheriff who transported the individual for evaluation.
- In response to a valid subpoena or court order of a court of competent jurisdiction***, EXCEPT*** for privileged information.

Privileged Communications

Individuals have a privilege to keep confidential the communications they make to their:

- Psychiatrist
- Licensed psychologist
- LCSW
- Clinical nurse specialist in psychiatric/mental health
- Licensed marriage and family therapist
- Licensed professional counselor

O.C.G.A. § 24-5-501, and § 43-39-16 for licensed psychologists

Privileged Communications

Additionally, communications between certain healthcare professionals who are providing/have provided psychotherapy to the individual, may be privileged.

- Only between the listed healthcare professionals.
- With a relationship to the individual.
- Regarding communications that are already privileged.

O.C.G.A. § 24-5-501(a)(8)

Privileged Communications

For the purposes of privilege, “psychotherapy” means providing psychotherapeutic techniques:

"Psychotherapeutic techniques" means those specific techniques involving the in-depth exploration and treatment of interpersonal and intrapersonal dynamics but shall not include the performance of those activities exclusively reserved to any other business or profession by any other chapter of [the Georgia professional code].

O.C.G.A. §§ 24-5-501(b); 43-10A-3(11)

Privileged Communications

When confidential mental health, developmental disabilities, or alcohol and drug abuse information CAN be disclosed to the following persons, Georgia law still prohibits disclosure to them of privileged communications that may be in the records. Privileged communications cannot be disclosed to:

- Coroners and medical examiners.
- Executors and administrators of a deceased individual's estate.
- Recipients of records via court order or subpoena.

O.C.G.A. §§ 37-3-166, 37-4-125, 37-7-166

Privileged Communications

- Privileged communications cannot be disclosed in a lawsuit.
- The individual can WAIVE the privilege.
- The healthcare professional/facility cannot waive the privilege.
- The privilege extends past the individual's death, and does not "die" with the individual.

Privileged Communication of Threats

If an individual is making threats to harm someone:

- The provider's first duty is to keep or make the individual secure, as appropriate under the law. Is involuntary status possible (danger to self *or* *others*)? Can the provider prevent an unsafe discharge?
- Does the treatment team know about the threat?
- Should the threat be disclosed?
  - All facts must be considered
  - Law in Georgia is not clear
  - DBHDD assumes that it is NOT okay to make a disclosure
  - Contact your attorney to gather and discuss all the facts, and to define your policy!

Authorization to Disclose PHI and Privileged Communications

An individual may authorize in writing for his/her PHI, including privileged communications, to be disclosed to a named person or facility.

- Does the individual have the mental "capacity" to authorize the disclosure?
  - Capacity means understanding what you are doing and the consequences of what you are doing.
  - Does the individual know what he/she is doing when he/she signs an authorization?
  - In DBHDD, the physician/treatment team determines whether an individual has capacity to sign an authorization to disclose PHI.

Georgia Law and HIPAA: Subpoenas

Ask your attorney about Georgia Law, especially regarding court orders and subpoenas for disclosure of PHI.

HIPAA requires notice to the individual if PHI is subpoenaed, or a "qualified protective order."

The individual may not have a way of knowing that his/her PHI is being sought in a lawsuit.

It may be advisable for an attorney to file a motion or take other legal action on behalf of the covered entity.

HIPAA: Covered Entities

Covered entity means:

1) A health plan,
2) A health care clearinghouse, OR
3) A health care provider who conducts financial and administrative transactions electronically, such as electronic billing and fund transfers.

KNOW whether you are a Covered Entity and whether HIPAA and this portion of the presentation apply to you!

45 C.F.R. § 160.103

HIPAA Basics: Identifying Individuals

HIPAA says that protected health information (PHI) is confidential when it identifies:

- The individual
- The individual's relatives
- The individual's employers OR
- The individual's household members

45 C.F.R. § 164.514(b)(2)(i)

HIPAA Basics: Identifying Individuals

If someone is requesting PHI but is not authorized to access PHI, and you know that the person has information about the individual, you can't disclose PHI to that person if they could:

- Use what they know
- To "make a match" and identify the individual.

45 C.F.R. § 164.514(b)(2)(ii)

Examples:

- People you know in the community already
- "Common acquaintances" of people you know

HIPAA Basics: Callers Seeking PHI

Because all information about individuals is confidential, DBHDD does not confirm or deny to a member of the public whether an individual is receiving or has received treatment or services.

DBHDD training says that if an individual's family/friends call:

- DBHDD staff say they cannot confirm or deny anything about an individual, even whether they are at the hospital or not.
- Staff politely end the conversation, hang up, and ask the individual:
  - If he/she wants to authorize the disclosure, or
  - If he/she will make a call back to the family/friend.

O.C.G.A. §§ 37-3-166, 37-4-125, 37-7-166

HIPAA Basics: Continuity of Care with DBHDD Hospitals

HIPAA requires that the covered entity verify the identity of a caller or person requesting PHI.

To speak with DBHDD hospital staff about a hospitalized individual whom you have treated or served, if there are questions on verification, send the DBHDD social services chief a copy of your "face sheet" on the individual. This documentation:

- Provides some verification of the caller's identity
- Provides evidence that the provider has a treatment relationship with the individual
- Facilitates continuity of care disclosures of information between provider and hospital.

45 C.F.R. §§ 164.514(h), 164.506(c). O.C.G.A. §37-3-166(a)(3)

HIPAA Basics: Minimum Necessary Rule

Staff who do not have duties regarding an individual should not have access to the individual's PHI.

When staff use or disclose PHI, they should use/disclose only the minimum PHI that is necessary to accomplish the purpose for which the use or disclosure is being made.

When providing treatment, the minimum necessary rule does not apply.

45 C.F.R. §§ 164.502(b), 164.514(d).

HIPAA Basics: Additional Rules

HIPAA also includes rules on:

- Confidentiality of Genetic Information
- Fundraising, Marketing and PHI
- Research and PHI
- Sale of PHI

Remember – *State law may be more strict on confidentiality*, so you may need to follow state law instead of HIPAA! Ask your attorney for guidance.

HIPAA Basics: Document Retention

Policies, required communications, and documentation of actions required by HIPAA are to be retained for "six years from the date of … creation, or the date when … last in effect, whichever is later."

Should documents be retained for a longer period of time?

Are employees deleting texts, e-mails, or voice mail messages too soon?

45 C.F.R. § 164.530

HIPAA Basics: Physical Security

- Does provider policy require shredding paper PHI before disposal?
- Are there locked recycling/trash bins for paper PHI?
- Does the provider have means of shredding or wiping electronic devices?
- Are photocopiers and scanners wiped before returning to the leasing company, or before disposal?
- Does you have occasion to deliver paper PHI, and is it “secure in transmission”?

HIPAA Basics: Physical Security
Clean Desk Practice

Unless you have an office with a door that you lock…

- Can you clear your desk of documents containing PHI before you leave work?
- Do you maintain PHI under lock and key?

And….

- Do you assign someone to monitor fax machines, copiers and meeting rooms for uncollected PHI?

Electronic PHI

What about electronic records?

A tangible copy of an electronic record is considered an “original” for purposes of disclosures.

O.C.G.A. § 31-33-8

Electronic Redaction

Certain information may need special authorization or legal basis for disclosure (alcohol or drug records, HIV/AIDS, privileged communications).

Consider the options if no authorization is obtained:

- Redact on paper (black out or white out) if necessary.
- This includes pixelating photos and videos to obscure the facial or other identity of an individual.
- Redact alcohol and drug information from mental health records, as needed, as well as HIV/AIDS information.

Electronic Accounts

- Is there a business e-mail account that all staff are required to use? Or are they using personal e-mail accounts (gmail, yahoo, hotmail, etc.)?
  - Difficulties in controlling and monitoring personal accounts
  - Inability of provider's Security Officer to verify security of personal accounts
- Is there an on-boarding and off-boarding process for hiring, internal transfers, and termination of staff accounts? Do staff avoid "mirror" access to accounts?
- Can accounts be audited?
- Same principles apply to databases and other electronic PHI.

Electronic Devices

"Security" under HIPAA includes physical and electronic security.

45 C.F.R. §§ 164.302 *et seq*.

- What devices are staff allowed to use? Does that include their personal devices? (BYOD policies)
- What policies do you have on physical security for devices? Are staff allowed to remove them from the workplace?
- Is the workplace physically secure, to protect devices?
- Are staff trained to not store passwords on sticky notes attached to the electronic device or nearby?

Personal Devices: Social Media Risks

- In our personal lives, why do we love e-mail, Facebook, Twitter, SnapChat, Instagram, and other social media? Sharing is:
  - Immediate
  - Widespread
  - Easy for others to share
  - Permanent

- Social media disclosure of PHI is risky and prohibited because it's:
  - Immediate
  - Widespread
  - Easy for others to re-disclose an individual's PHI without authorization
  - Permanent

Personal Phones and Devices

DBHDD prohibits use of staff's personal cell phone on the unit, or in the presence of individuals or their family members.

- This reduces the risk of PHI getting onto or being transmitted by a personal device, even accidentally. PHI is for DBHDD devices only!
- DBHDD issues a department-owned cell phone or laptop if staff need it for DBHDD work.

Use of Wireless Communication Devices in DBHDD Hospitals, 03-702 :: PolicyStat

Where to save PHI?

Consider whether your electronic storage of PHI is secure.

- Is the device/account password protected?
- Is a password stored on or near the device?
- Is there PHI on the desktop, immediately accessible?
- Is PHI in the “Notes” section of a smart phone?
- If PHI is in an app or web-based portal, is the app/portal secure (password protected, etc.)?
- Consider establishing direct access to your network via VPN when operating remotely, for secure access to e-PHI.

E-mail and PHI

Is PHI "safe in transmission" electronically?

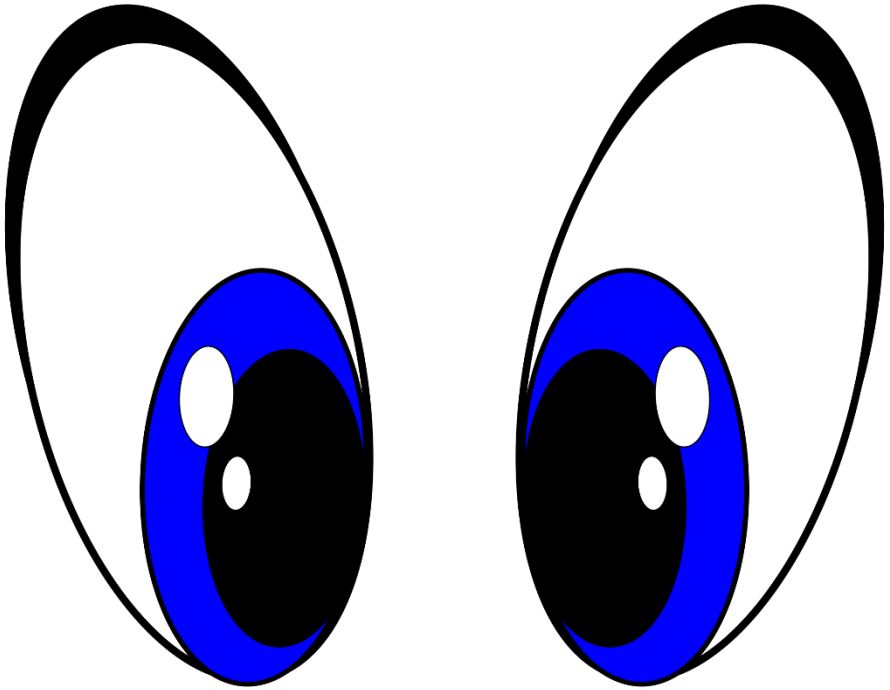
- Encryption of devices is an "addressable" standard
- It provides a "safe harbor" against a HIPAA breach – if a device is lost or stolen, there is likely no breach if the device is encrypted.
- Alternatives?
  - Use a secure web portal that is password-protected
  - Send documents that are "zipped" and send the password in a separate e-mail
  - Check with your Security Official.

45 C.F.R. § 164.312

E-mail Security Training

- In phishing e-mails, an attacker tries to learn login credentials or account information by masquerading as a reputable entity or person. Don't open the e-mail.
- Don't forward chain e-mails.
- Be cautious about links, attachments, and images in e-mails. Don't open them if you don't know and trust the sender.
- Don't share passwords with anyone, even your helpdesk staff.
- REPORT security issues to your Security Officer!!

Caution! Stay Alert!



Emails: check before you send

- Is everyone is your Contacts or Address Book authorized to receive PHI? (Note: a risk factor of personal devices.)
- CHECK to see if all recipients are authorized to receive the PHI you are sending.
- CHECK to see if there is PHI in the previous e-mail chain or attachments that others may have included.
- CHECK to see if you have the correct name and address for all recipients.
- Have a process in place to correct mis-delivered e-mails.

Pay attention – Avoid Human Error

- When discussing PHI, are there other individuals, visitors, or any unauthorized persons within earshot?
- When leaving phone messages, are staff disclosing PHI to whoever picks up the message?
- Are you sure that the provider is authorized to disclose information to family, visitors, providers?
- Did you leave any of your paperwork behind when you left a meeting or other event?

Mistakes - Identity

- Did you check the authorization and the address of the person to whom you are mailing documents?
- Did you check documents before you give them to an individual - does the PHI belong to them?
- Did you check all details of e-mails (identity, authorization, addresses, etc.) before hitting "send"?
- Did you verify the identity of the person who is calling or visiting?

Mistaken Identity

What are your procedures to check and re-check identities in documenting and in disclosing PHI?

Sanctions

HIPAA requires that the covered entity bring sanctions against employees who violate HIPAA.

A court or a federal enforcement agency may impose criminal monetary penalties or incarceration for breaches of HIPAA.

45 C.F.R. § 164.530

Georgia Health Information Network (GaHIN)

DBHDD belongs to GaHIN for electronic disclosure of its discharge summary data to other GaHIN members:

- ONLY for individuals who authorize in writing on an OPT-IN basis.
- Disclosures will include alcohol and drug information disclosures by authorization. Electronically redacting this information is not available at present, so authorization is required.
- Disclosures are to current and FUTURE providers for 1 year.
- GaHIN members include medical providers as well as behavioral health providers.
- Most other GaHIN members' policy is for individuals to OPT-OUT.

Georgia Health Information Network (GaHIN)

Providers are urged to consider joining GaHIN on an

OPT-IN basis only, if they join, so that individuals must sign an authorization for disclosures through GaHIN.

Alcohol and drug abuse information is particularly confidential and requires authorization for disclosure. Consider your policies and procedures carefully.

Other health information networks or exchanges will likely present the same issues.

Consult your attorney!

Confidentiality and HIPAA

THANKS for your time and attention!