# CONFIDENTIALITY AND HIPAA

Presented to DBHDD Providers
By Elizabeth Bentley Watson
DBHDD Attorney and HIPAA Privacy Officer
betty.bentley.watson@dbhdd.ga.gov
August 2014

#### Disclaimer

- This presentation does not constitute legal advice.
- Providers should seek their own legal advice from their own counsel 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 applicable laws!

## **Confidentiality Count\$!**

Federal civil monetary penalties by the U.S. Department of Health and Human Services have ranged from:

\$35,000

To

\$4.3 Million!!

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

<u>See</u> handout on "United States Health and Human Services "Resolution Agreements" Regarding HIPAA Violations.

#### **Topics for Presentation**

- Various Confidentiality Laws and HIPAA
- Eight (8) of the HIPAA procedural "bells and whistles"
- General disclosure practices
- Risk prevention issues

See also: Citations in the slides and on handouts

## Why Confidentiality?

- To prevent stigma
  - Negative impacts in employment, relationships, economic status, even possible criminal charges.
- Trust in treatment relationship
- 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 records
- Letters, court orders
- Conversations
- E-mails

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.

### "It's not just HIPAA!!"

Which law is the <u>least</u> strict on confidentiality??

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

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)
- Specific authority in the regulations
- Records CANNOT be produced in response to a subpoena!

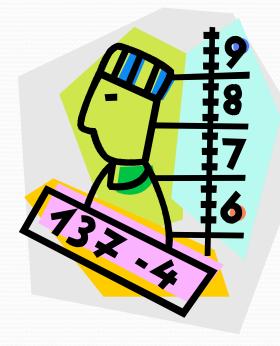
42 C.F.R. Part 2

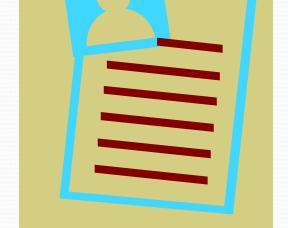
"Identifying an Individual":

Alcohol and drug information...



may incriminate!





- What is the name of your facility?
- Does your facility "hold itself out" as providing alcohol and drug abuse treatment?

What does the fact of admission to or treatment in your facility say about the individual?

Your facility may have to follow the strictest confidentiality rules!

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.



#### 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

#### **Georgia Laws**

Confidentiality of <u>mental health</u> and <u>developmental disabilities</u> 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 – Disclosures allowed

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/executor or other legal representative of the estate AND in response to a subpoena by the coroner or medical examiner

#### Georgia Laws – Disclosures allowed

Lawful disclosures, continued:

- For crimes alleged to occur on program premises, law enforcement may obtain circumstances of the incident
- For crimes elsewhere, law enforcement may know whether individual was hospitalized, and obtain last known address of individual
- Upon request and authorization by the individual, notice of discharge of adult involuntary individual may be given to sheriff who transported individual for admission.
- In response to a valid subpoena or court order of a court of competent jurisdiction, except for privileged information.

#### So what does HIPAA do??

HIPAA adds procedural bells and whistles -





#### **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 presentation apply to you!

45 C.F.R. § 160.103

### 1. Notice of Privacy Practices

"Notice of Privacy Practices" describes Individuals' **RIGHTS,** and how your program uses protected health information.



45 C.F.R. § 164.520 DBHDD Policy 23-101 "Notice of Privacy Practices"

### 1. Notice of Privacy Practices

Make good faith efforts to obtain a written acknowledgment of receipt of the Notice, even when it is given electronically.

Individuals, parents of minor individuals, guardians are ALL entitled to receive the Notice on request.

Notice must be POSTED prominently where it's likely individuals will see it.

45 C.F.R. § 164.520

## 2. "Privacy Official"

Health care providers need a designated <u>Privacy Official</u> whose job is to:

- 1. Implement confidentiality policies and procedures.
- 2. Receive and handle privacy complaints.
- Provide information about your Notice of Privacy Practices.

45 C.F.R. § 164.530(a)

## 3. Authorization Form – Section on Special Confidentiality

#### AUTHORIZATION FOR RELEASE OF INFORMATION

I authorize the disclosure of alcohol or drug Initials abuse information, if any.

I authorize the disclosure of information, if Initials any, concerning testing for HIV and/or treatment for HIV or AIDS and any related conditions.

45 C.F.R. § 164.508; 42 C.F.R. Part 2 DBHDD Policy 23-100, See Attachment B for the complete form

#### 4. Individual's Rights

- To access his/her own PHI (clinical records).
- To <u>request</u> that the provider:
  - Limit the use or disclosure of his/her PHI.
  - Restrict the persons to whom disclosure may be made.
  - Amend PHI in his/her clinical record.
- To obtain an "Accounting of Disclosures" of his/her PHI.

45 C.F.R. §§ 164.522 – 164.528

DBHDD Policy 23-105 "Rights of Individuals Regarding Their Confidential and Protected Health Information"

### 4. Individual's Rights

Request restriction of access by others to his/her records.

\*\*\*\* New regulation — if individual "pays in full" for services, provider must agree to the restriction.

#### 4. Individual's Rights

An individual has the right to review of a denial of access if:

A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual. This restriction applies only to individuals who are currently being treated by the facility or program from which they are requesting records.

45 C.F.R. § 164.524(a)(3) AND Georgia Regulations 290-4-6-.05(3).

#### 5. Complaints

<u>Anyone</u> can file a Complaint with a provider about confidentiality rights.

- The health care provider may not retaliate against an employee who makes a complaint.
- Designate which staff will receive complaint forms.
- Individuals may also complain to the United States
   Department of Health & Human Services.

45 C.F.R. §§ 164.530(d); 160.306(a).

DBHDD Policy 23-103, "Confidentiality and HIPAA Privacy Complaints" and Attachment B, "Privacy Complaint Report Form"

#### 6. Business Associates

#### **Business Associate:**

A person or entity who, on behalf of the health care provider, creates, receives, maintains or transmits PHI for a function such as claims processing, data analysis, utilization review, quality assurance, etc. OR who provides legal, actuarial, accounting, consulting, data aggregation, financial services, etc. that require access to PHI, to or for the provider.

45 C.F.R. § 160.103

DBHDD Policy 23-107, "Confidentiality and HIPAA Practices Involving Business Associates"

#### 6. Business Associates

HIPAA requires providers to have Business Associate Agreements with all Business Associates:

Business Associate Agreements must obtain "satisfactory assurances" that the Business Associate will appropriately safeguard PHI.

Business Associates must obtain Business Associates with ALL their subcontractors that must access PHI.

45 C.F.R. §§ 164.502 and 164.504.

DBHDD Policy 23-107, "Confidentiality and HIPAA Practices Involving Business Associates"



What happens if...

"Mistakes were made"?

#### **DBHDD Policies and Procedures:**

- Who must report?
- What must be reported?
- When (how quickly) must you report?
- Where (to whom) is a report sent?
- Who will investigate?
- Violation Report form

45 C.F.R. § 164.400 – 164.414

DBHDD Policy 23-102, "Reporting and Notification of Breaches of Confidentiality" and Attachment A "Privacy Violation Report Form."

If you are a Business Associate of DBHDD, you must report HIPAA violations to DBHDD.

If you have Business Associates of your own, HIPAA requires that your have your Business Associates report their violations to you.

DBHDD monitors confidentiality and HIPAA violations of Providers through contract compliance and corrective action plans, etc.

45 C.F.R. § 164.400; 164.410; 164.504(e)(2).

DBHDD Policy 23-107, "Confidentiality and HIPAA Practices Involving Business Associates"

**Breach** – Not all violations of HIPAA are "breaches."

A violation of HIPAA is a breach if it also meets the following definition: The acquisition, use or disclosure of protected health information (PHI) in a manner not permitted by HIPAA, which *compromises the security or privacy* of the PHI.

45 C.F.R. § 164.402

HIPAA <u>presumes</u> that all violations are breaches unless the covered entity proves otherwise through a <u>Risk</u> <u>Assessment</u> that is described in HIPAA regulations.

#### Practice tip:

The DBHDD Privacy Violation Report Form includes the steps for the Risk Assessment.

45 C.F.R. § 164.402

DBHDD Policy 23-102, "Reporting and Notification of Breaches of Confidentiality" and Attachment A "Privacy Violation Report Form."

HIPAA requires **notification** of the breach:

- to the individual
- to the United States Department of Health and Human Services, and
- IF the breach involved disclosure of over 500 individuals' information, to the media.

45 C.F.R. § 164.404 – 164.408

Reporting to HHS is done online in the first 60 days of the calendar year, for breaches in the previous calendar year.

#### Practice Tip:

The DBHDD Violation Report Form is modeled on the HHS online reporting page. Providers are free to copy the DBHDD form for their own use.

DBHDD Policy 23-102, "Reporting and Notification of Breaches of Confidentiality."

#### 8. Sanctions

HIPAA requires that the covered entity (provider) 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

#### **General: Disclosures**

After a disclosure is made:

The information is *still confidential!* 

Disclosure to Ms. A that is valid under the law does <u>not</u> authorize disclosure to Mr. B, C, or D.

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

# **General – Disclosures via Subpoenas and Court Orders**

Ask your attorney about Georgia Law.

Also: HIPAA requires notice to the individual if PHI is subpoenaed.

Would an individual want to know – and object - if his/her mental illness or developmental disability records were sought by subpoena:

- In a divorce case?
- In a child custody case?
- If the individual was the victim of a crime?

## **General: Disclosures**

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

## **General: Disclosures**

Certain information may need special authorization or legal basis for disclosure.

#### Options if no authorization is possible:

- Redact (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.

#### **New HIPAA Rules in 2013**

NEW Omnibus HIPAA Rule (January 25, 2013):

http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

#### New rules on:

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

BUT – <u>State law remains unchanged</u> and you may need to follow state law instead of HIPAA!!

#### **Risk Prevention**

#### Some risks to prevent:

- 1. Electronic devices containing PHI loss or theft of flash drives, laptops, smart phones, tablets.
- 2. E-mails to the wrong person.
- Lack of attention to conversations and documents.
- Loss of documents.
- 5. Improper disposal of PHI in regular trash, not shredded.

# E-mails – <u>check</u> before you send!

- Is everyone is your Contacts or Address Book <u>authorized</u> to receive PHI??
- Can you obtain <u>encryption</u> of e-mails?
- 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.

# Pay attention!

- When <u>discussing PHI</u>, are there other individuals, visitors, or any unauthorized persons within earshot?
- When leaving <u>phone messages</u>, are you disclosing PHI to whoever picks up the message?
- Are you sure that you are <u>authorized</u> to disclose information to family, visitors, providers?
- Did you leave any of <u>your paperwork</u> behind when you left a meeting or other event?
- Did you check the authorization and the address of the person to whom you are <u>mailing documents</u>?

#### **Clean Desk Practice**

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

And especially if you work at a residential services location:

- Clear your desk of documents containing PHI before you leave work.
- Keep PHI under lock and key.
- Assign someone to monitor fax machines, copiers and meeting rooms – don't leave PHI uncollected.

## **CONFIDENTIALITY AND HIPAA**



## **CONFIDENTIALITY AND HIPAA**

Thanks for your time and attention!