

HIPAA and Confidentiality



DBHDD

**To Share or Not to Share?
DBHDD Behavioral Health
Symposium
Brenda King Woodard, Esq.
DBHDD Director, Legal Services
October 5, 2017**

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!

Topics for Presentation

- HIPAA
- Georgia laws regarding protected health information
- Substance Use federal laws regarding protected health information
- Risk Prevention
- Sanctions

HIPAA

SECTION OVERVIEW
WHAT IS HIPAA
HIPAA BASICS

WHAT IS HIPAA?

- HIPAA, or the Health Insurance Portability and Accountability Act of 1996
- United States legislation that provides data privacy and security provisions for safeguarding medical information
- Gives patients more control over their health information
- Sets boundaries on the use and release of health records

HIPAA Basics: Covered Entities

- Those who must comply with HIPAA are often called HIPAA-covered entities
- Covered entity means:
 - A health plan,
 - A health care clearinghouse, OR
 - A health care provider who transmits any health information in electronic form in connection with a covered transaction (such as electronic billing and fund transfers)
- **KNOW** whether you are a Covered Entity and whether HIPAA applies to you!

45 C.F.R. § 160.103

HIPAA Basics: Covered Entities

- For HIPAA purposes, health plans include:
- Health insurance companies
- HMOs, or health maintenance organizations
- Employer-sponsored health plans
- Government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs

HIPAA Basics: Covered Entities

- For HIPAA purposes, Clearinghouses are organizations that process nonstandard health information to conform to standards for data content or format, or vice versa, on behalf of other organizations
- Examples include a repricing company billing service, community health management information system, community health information system

HIPAA Basics: Covered Entities

- Providers who submit HIPAA transactions, like claims, electronically are covered entities and include but are not limited to:
 - Doctors
 - Clinics
 - Psychologists
 - Dentists
 - Chiropractors
 - Nursing homes
 - Pharmacies

HIPAA Basics: 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. 45 C.F.R. § 164.304

HIPAA-speak: “Protected Health Information (PHI)”

Protected health information means individually identifiable health information 45 C.F.R. § 160.103

See DBHDD Policy 23-100 “Confidentiality and HIPAA”

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: Confidentiality and HIPAA

ALL information about individuals is confidential regardless of the format!!

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

45 C.F.R. § 160.103

HIPAA Basics: 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

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: 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: Does HIPAA Apply

- The general standard: if a state law or another law is more protective of the patient, then it takes precedence over HIPAA
- If you are not sure, ask your attorney for guidance!

HIPAA Basics: Additional Rules

HIPAA also includes rules on:

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



GEORGIA LAWS

SECTION OVERVIEW
CONFIDENTIALITY OF MH AND DD PHI
LAWFUL DISCLOSURES
PRIVILEGED COMMUNICATIONS
DISCLOSURES

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: Lawful Disclosures

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

Georgia Laws: Lawful Disclosures

- 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
- 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

Georgia Laws: Lawful Disclosures

- 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

Georgia Laws: Lawful Disclosures

- 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

Georgia Laws: 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

Georgia Laws: 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)

Georgia Laws: 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)

Georgia Laws: 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

Georgia Laws: 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

Georgia Laws: Privileged Communications

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!

Georgia Laws: 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 Laws: 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)

Scenario: Callers Seeking PHI

Maggie is a patient who is currently in a state hospital receiving treatment for mental illness. Worried about Maggie, Maggie's sister, Sarah, calls DBHDD asking if her sister is currently receiving services.

Is it appropriate for DBHDD to simply inform Sarah that Maggie is in fact receiving treatment, as long as no other information is disclosed?



Scenario: Callers Seeking PHI

Answer:

No. 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.



Scenario: Callers Seeking PHI

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

SUBSTANCE USE FEDERAL LAWS

SECTION OVERVIEW SUBSTANCE USE REGULATIONS RECENT CHANGES TO SAMHSA REGULATIONS

Federal Regulations: Confidentiality of Substance Use Disorder Patient Records

Records and information *identifying an individual* as having a substance use disorder 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.
- Substance use records **CANNOT** be produced in response to a subpoena!

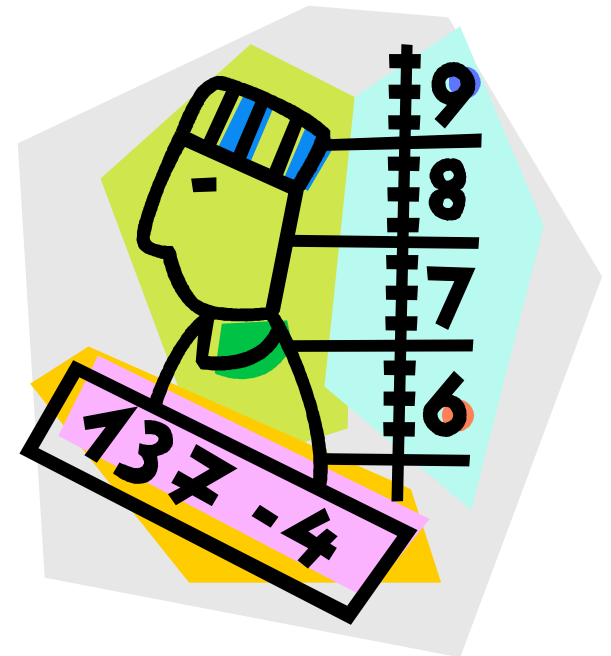
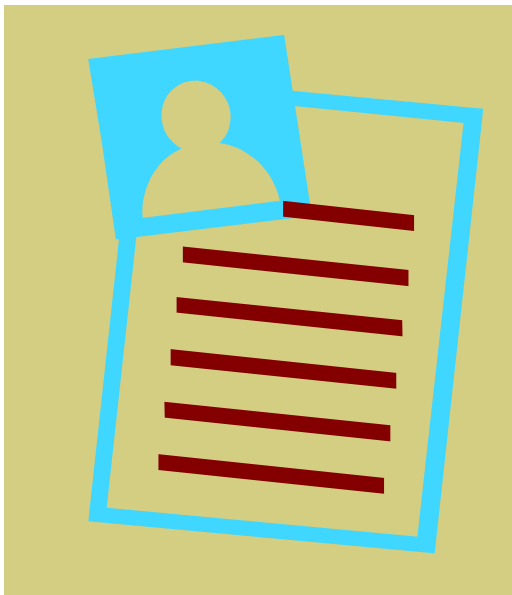
42 C.F.R. Part 2

Federal Regulations: Confidentiality of Substance Use Disorder Patient Records

“Identifying an Individual”:

Substance use information...

may incriminate!



Federal Regulations: Confidentiality of Substance Use Disorder Patient Records

Substance use disorder 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 Substance Use Disorder Patient Records



CONFIDENTIAL AND PRIVILEGED

This information has been disclosed to you from records protected by federal confidentiality rules (*42 CFR part 2*). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR 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 investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§ 2.12(c)(5) and 2.65.

42 C.F.R. § 2.32 (emphasis added)

Recent Changes to SAMHSA Regulations: 42 C.F.R. part 2

- **Reports of Violations (§ 2.4)** reporting a violation of these regulations by methadone programs (now referred to as opioid treatment programs) is now to be reported to the Food and Drug Administration (FDA)
- **Confidentiality Restrictions and Safeguards (§ 2.13)** has a new requirement that, upon request, patients who have included a general designation in the “To Whom” section of their consent form must be provided a list of entities (referred to as a List of Disclosures) to which their information has been disclosed pursuant to the general designation
- **Security for Records (§ 2.16)** clarifies that this section requires both part 2 programs and other lawful holders of patient identifying information to have in place formal policies and procedures addressing security, including sanitization of associated media, for both paper and electronic records

Recent Changes to SAMHSA Regulations: 42 C.F.R. part 2

- **Disposition of Records by Discontinued Programs (§ 2.19)** addresses both paper and electronic records. SAMHSA also added requirements for sanitizing associated media.
- **Notice to Patients of Federal Confidentiality Requirements (§ 2.22)** SAMHSA clarifies that the written summary of federal law and regulations may be provided to patients in either paper or electronic format. SAMHSA also revised § 2.22 to require the statement regarding the reporting of violations include contact information for the appropriate authorities.
- **Consent Requirements (§ 2.31)** permits, in certain circumstances, a patient to include a general designation in the “To Whom” section of the consent form, in conjunction with requirements that the consent form include an explicit description of the amount and kind of substance use disorder treatment information that may be disclosed. SAMHSA also revised § 2.31 to require the part 2 program or other lawful holder of patient identifying information to include a statement on the consent form when using a general designation in the “To Whom” section of the consent form that patients have a right to obtain, upon request, a list of entities to which their information has been disclosed pursuant to the general designation. SAMHSA also revised § 2.31 to permit electronic signatures to the extent that they are not prohibited by any applicable law.

Recent Changes to SAMHSA Regulations: 42 C.F.R. part 2

- **Prohibition on Re-disclosure (§ 2.32)** SAMHSA clarifies that the prohibition on re-disclosure only applies to information that would identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment for a substance use disorder, such as indicated through standard medical codes, descriptive language, or both, and allows other health-related information shared by the part 2 program to be re-disclosed, if permissible under other applicable laws.
- **Medical Emergencies (§ 2.51)** revises the medical emergency exception to make it consistent with the statutory language and to give providers more discretion to determine when a “bona fide medical emergency” exists.

Recent Changes to SAMHSA Regulations: 42 C.F.R. part 2

- **Research (§ 2.52)** SAMHSA revises the research exception to permit data protected by 42 CFR part 2 to be disclosed to qualified personnel for the purpose of conducting research by a part 2 program or any other individual or entity that is in lawful possession of part 2 data if the researcher provides documentation of meeting certain requirements related to existing protections for human research. SAMHSA also revised § 2.52 to address data linkages to enable researchers holding part 2 data to obtain linkages to other datasets, provided that appropriate safeguards are in place.
- **Audit and Evaluation (§ 2.53)** the update modernizes the requirements to include provisions governing both paper and electronic patient records. SAMHSA also revised § 2.53 to permit an audit or necessary evaluation to meet the requirements of a Centers for Medicare & Medicaid Services (CMS)-regulated accountable care organization (CMS-regulated ACO) or similar CMS-regulated organization (including a CMS-regulated Qualified Entity (QE)), under certain conditions.

REVIEW

Laws in order of protection of patients

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

Scenario: Applying PHI Rules

Sam, a patient at XYZ Drug Treatment Program, is involved in a major heroin distribution ring and has been distributing drugs to other patients.

Can Sam's program tell the police and release information to the prosecutor?



Scenario: Applying PHI Rules

Answer

Yes. Both the HIPAA Privacy Rule (§164.152(f)(5), (6)) and 42 CFR part 2 (§2.12(c)(5)) allow a program to report patient crimes on its premises to law enforcement.



RISK PREVENTION

SECTION OVERVIEW
SECURITY
COMMON MISTAKES

Risk Prevention: Security

“Security” under HIPAA includes:

- Physical security of PHI
- Electronic security of PHI

45 C.F.R. §§ 164.302 *et seq.*

Risk Prevention: 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?
- Do you have occasion to deliver paper PHI, and is it “secure in transmission”?

Risk Prevention: Physical Security

- 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?

Risk Prevention: Physical Security

- Do you have a 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?
- Do you assign someone to monitor fax machines, copiers and meeting rooms for uncollected PHI?
- When discussing PHI, are there other individuals, visitors, or any unauthorized persons within earshot?

Risk Prevention: Electronic Security

- 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.)?
- Is there an on-boarding and off-boarding process for hiring, internal transfers, and termination of staff accounts?
- Can accounts be audited?
- Same principles apply to databases and other electronic PHI

Risk Prevention: Electronic Security

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

Risk Prevention: Electronic Security

- Is everyone in your Contacts or Address Book authorized to receive PHI?
- 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

Risk Prevention: Common Mistakes

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



Risk Prevention: Common Mistakes

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

- When leaving phone messages, are staff disclosing PHI to whoever picks up the message?
- How do you verify the caller's identity?
- Do you obtain evidence that the provider has a treatment relationship with the individual?

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

Risk Prevention: Common Mistakes

- Did you check the authorization and the address of the person to whom you are mailing documents?
- Did you check documents before you gave 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?

Risk Prevention: Common Mistakes

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

Risk Prevention: Common Mistakes

Be Smart with Redaction!

It is not enough to highlight text in black or cover the information with a colored rectangle. These methods work for hard copy documents, but they are not appropriate for electronic documents. To remove the information, you should

While simply highlighting a document in black can initially appear to cover protected health information electronically, 


Risk Prevention: Common Mistakes

While simply highlighting a document in black can initially appear to cover protected health information electronically, by simply clicking the “tools section” in a PDF and changing the font color to “white,” you can instantly see all of the “hidden” information.

**BE
CAREFUL**

SANCTIONS

SECTION OVERVIEW
TYPES OF SANCTIONS
EXAMPLES OF SANCTIONS

Sanctions: Types of Sanctions

- HIPAA Violations may result in civil sanctions including monetary fines
- HIPAA Violations may result in criminal sanctions including incarceration and payment of monetary fines
- Penalties have ranged from **\$25,000-\$5.55 Million**
- Requires that the covered entity bring sanctions against employees who violate HIPAA

45 C.F.R. § 164.530



Sanctions: Examples of Sanctions

- The \$5.5 Million Mistake-Memorial Healthcare System 2017
- The PHI of 115,143 individuals had been impermissibly accessed by hospital employees, and was impermissibly disclosed to affiliated physician office staff.
- Additionally, the login credentials of a former employee had been used to access ePHI on a daily basis without detection from April 2011 to April 2012.
- The hospital failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. They also failed to review records of activity on applications that maintain ePHI.

See more at <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>

Sanctions: Examples of Sanctions

Being Nosey Can Cost You

UC Los Angeles Health System (2011)

Employees repeatedly, and without permissible reason, looked at electronic protected health information of two celebrity patients and numerous others. As a result, the health system paid \$865,500 in fines for this breach of confidentiality.



Sanctions: Examples of Sanctions

Proper Policies Can Save Big Money!

Hospice of North Idaho (2012)

An unencrypted laptop containing PHI was stolen, which contained information of 441 individuals. There were no policies regarding mobile device security and no risk analysis. This theft cost the hospice \$50,000.

Affinity Health Plan, New York (2013)

The hard drive from a photocopier was sold to CBS Evening News without the PHI of 344,579 individuals being erased. There were no policies and procedures governing the return of photocopiers to leasing agents. The agency paid \$1,215,780 in fees.

WellPoint, Inc. Managed Care (2013)

An online application database containing PHI was accessible to unauthorized persons over the internet. The care center had inadequate policies and procedures on authorizing access to the database, and there were no technical safeguards to verify those seeking access. This cost WellPoint \$1.7 million.

THANKS for your time and attention!

감사합니다 Natick
Danke Ευχαριστίες Dalu
Grazie Thank You Köszönöm
Спасибо Dank Gracias
谢谢 Merci Seé
ありがとう

Obrigado