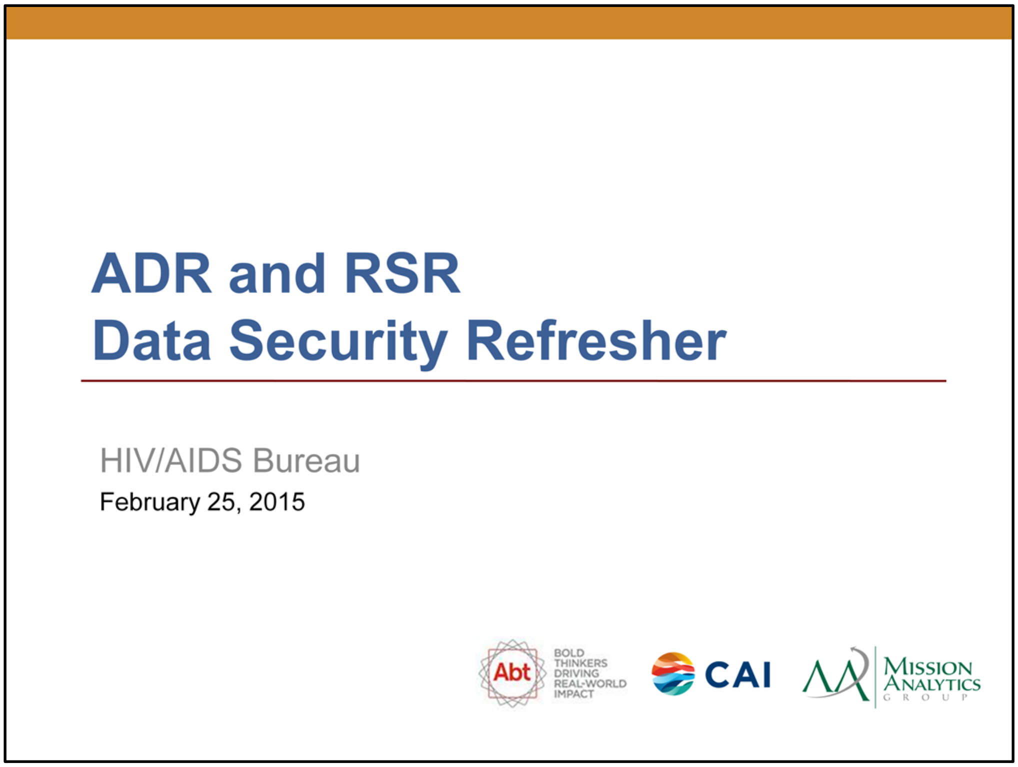


ADR and RSR Data Security Refresher

HIV/AIDS Bureau

February 25, 2015

Abt BOLD THINKERS DRIVING REAL-WORLD IMPACT · CAI · MISSION ANALYTICS GROUP

Welcome to today’s Webcast. Thank you so much for joining us today!

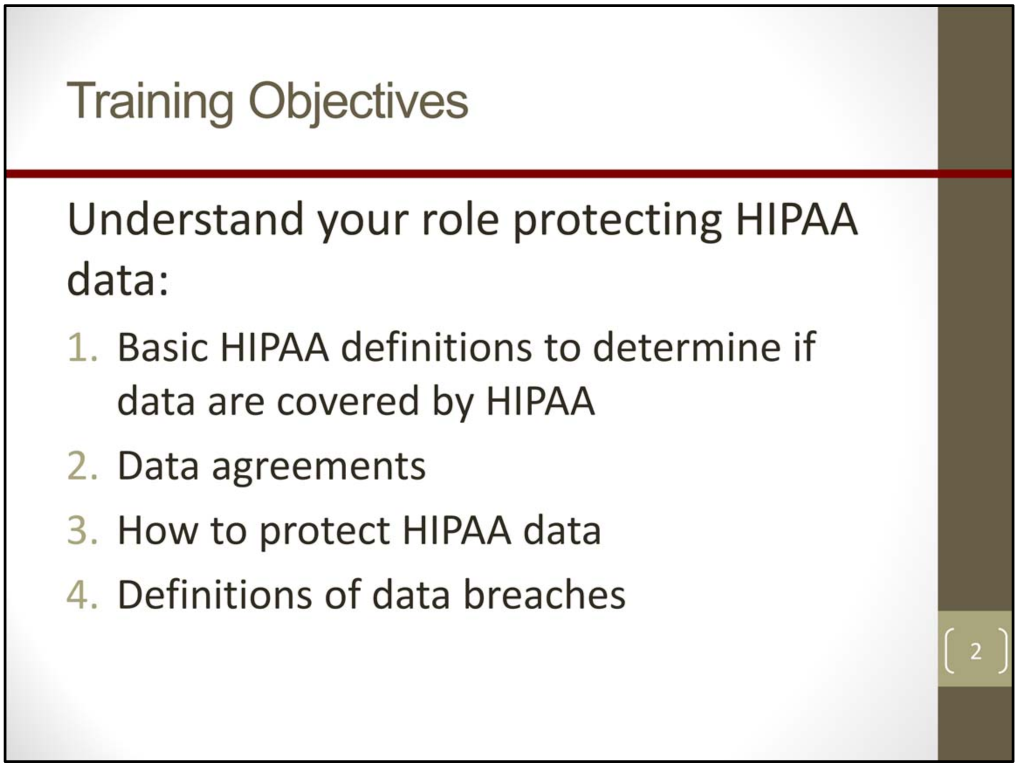
My name is Ellie Coombs. I’m a member of the DART Team, one of several groups engaged by HAB to provide training and technical assistance to Ryan White grantees during the implementation of the RSR and ADR.

Today’s Webcast is presented by Michael, also from the DART Team. Michael will provide an overview of the data security concerns of which all Ryan White HIV/AIDS Program grantees should be aware. Joining us for the question and answer portion is Theresa Doksum. Dr. Doksum serves as the Abt Associates IRB Chairperson and Research Integrity Officer.

At any time during the presentation, you’ll be able to send us questions using the “Question” function on your control panel on the right-hand side of the screen. You’ll also be able to ask questions directly “live” at the end of the presentation. You can do by clicking the “raise hand” button (on your control panel) and my colleague, Debbie, will conference you in. You can also click the “telephone” button and you’ll see a dial-in number and code.

We hope you consider asking questions “live,” because we really like hearing voices other than our own.

Now I’ll turn this over to our presenter, Michael.

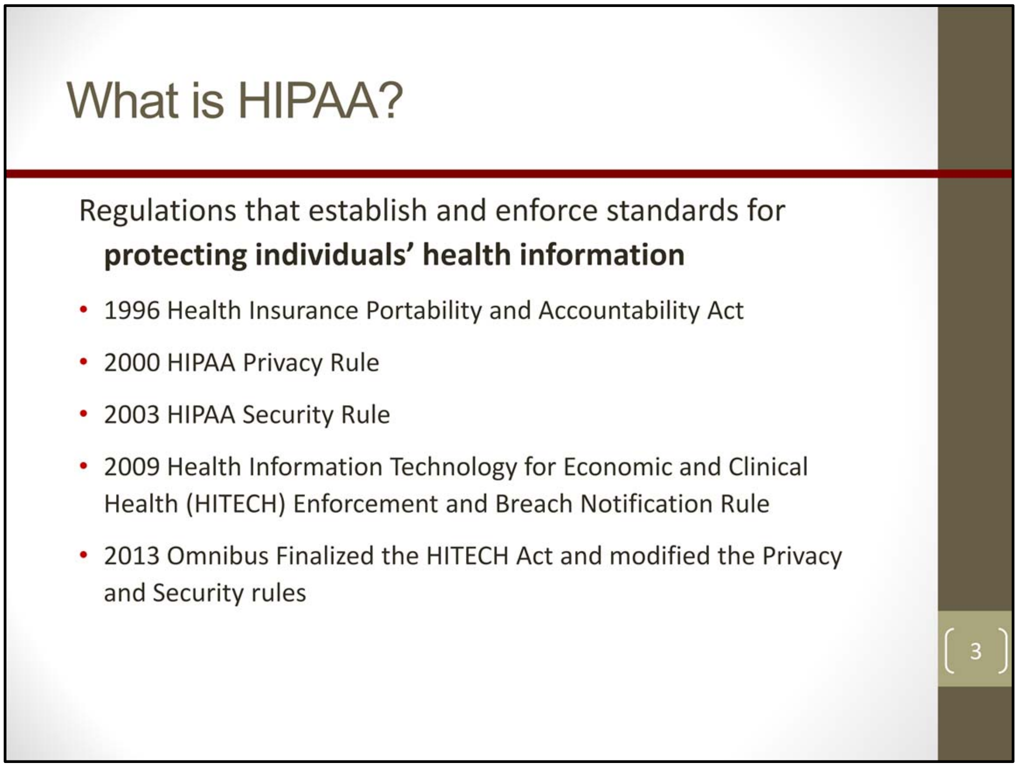


Training Objectives

Understand your role protecting HIPAA data:

1. Basic HIPAA definitions to determine if data are covered by HIPAA
2. Data agreements
3. How to protect HIPAA data
4. Definitions of data breaches

Today’s presentation will overview what data security requirements are involved in the RSR and ADR. These requirements are primarily governed by HIPAA, which we will review. We will also discuss how to go about maintaining and sharing data in a manner that ensures data are protected. In addition, we will explore what constitutes an actual data breach. Lastly, we will take your questions to clarify any points you want explore further.



What is HIPAA?

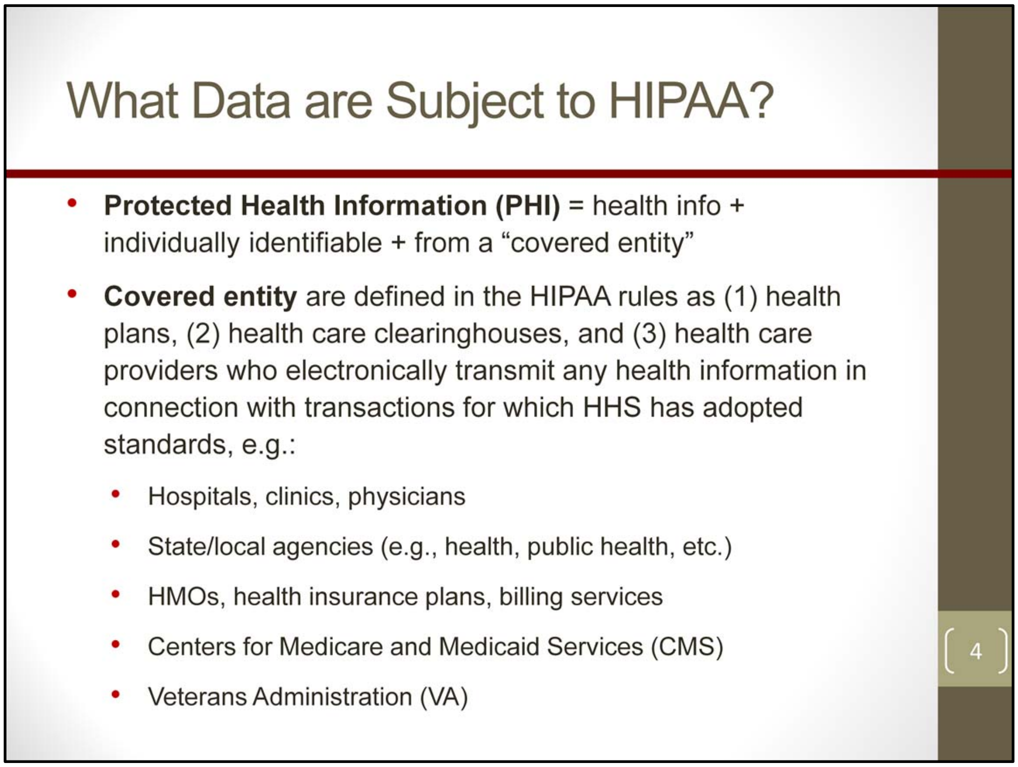
Regulations that establish and enforce standards for **protecting individuals' health information**

- 1996 Health Insurance Portability and Accountability Act
- 2000 HIPAA Privacy Rule
- 2003 HIPAA Security Rule
- 2009 Health Information Technology for Economic and Clinical Health (HITECH) Enforcement and Breach Notification Rule
- 2013 Omnibus Finalized the HITECH Act and modified the Privacy and Security rules

3

The Health Insurance Portability and Accountability Act, or HIPAA, governs many of the data security requirements surrounding RSR data.

HIPAA was fist enacted in 1996. Since that time it has experienced several major upgrades, affecting both data content as well as the media in which data are held. This webcast will not focus on the minute details of each of these rules and modifications; rather, what is most important to know is that each of these modifications has gradually strengthened the protection of PHI. It is also important to know that the Health Information Technology for Economic and Clinical Health (HITECH) Enforcement and Breach Notification Rule rule added penalties for violations of protections, particularly those that lead to data breaches – will discuss this more in later slides.

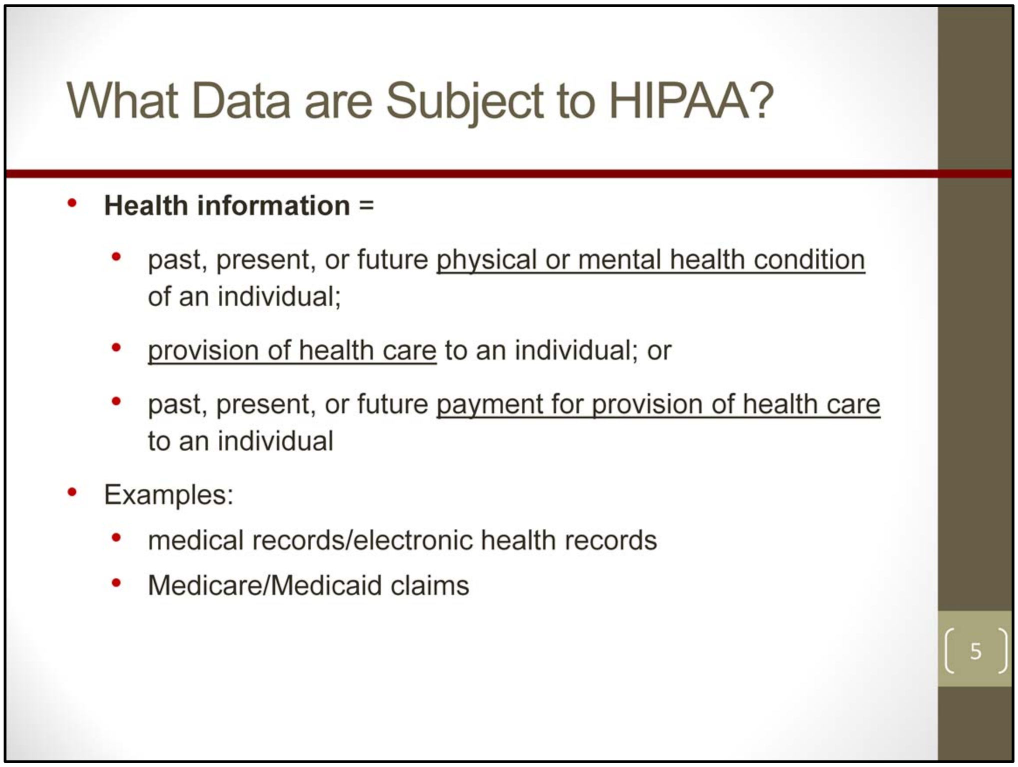


What Data are Subject to HIPAA?

- **Protected Health Information (PHI)** = health info + individually identifiable + from a “covered entity”
- **Covered entity** are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards, e.g.:
  - Hospitals, clinics, physicians
  - State/local agencies (e.g., health, public health, etc.)
  - HMOs, health insurance plans, billing services
  - Centers for Medicare and Medicaid Services (CMS)
  - Veterans Administration (VA)

While nearly all of you are likely well aware of HIPAA, it is always a good idea to start with a quick reminder of the kinds of data it governs. For our purposes we are focused on the collection, management and reporting of RSR data considered to be Protected Health Information, often referred to as PHI. PHI is clinical and medical service data from a covered entity that can be attributed to an identifiable individual.

Covered entities include health plans, health care clearing houses and health care providers. Health care clearing houses refer to entities such as billing and claims processing services, and benefit management organizations – examples include a clinic’s billing services subcontractor or a pharmacy benefits manager.

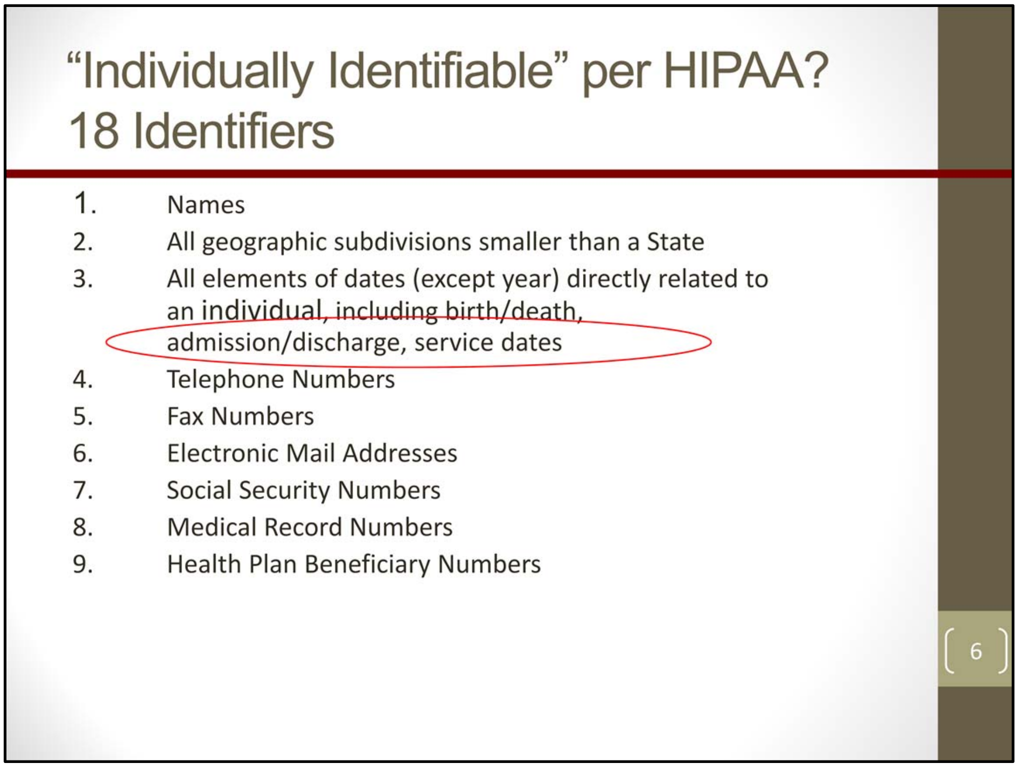


What Data are Subject to HIPAA?

- **Health information** =
  - past, present, or future physical or mental health condition of an individual;
  - provision of health care to an individual; or
  - past, present, or future payment for provision of health care to an individual
- Examples:
  - medical records/electronic health records
  - Medicare/Medicaid claims

So then what is health information? It is information about and individuals physical of mental health condition, health care services received and/or health care payment information.

Examples of these includes health record data and claims information.

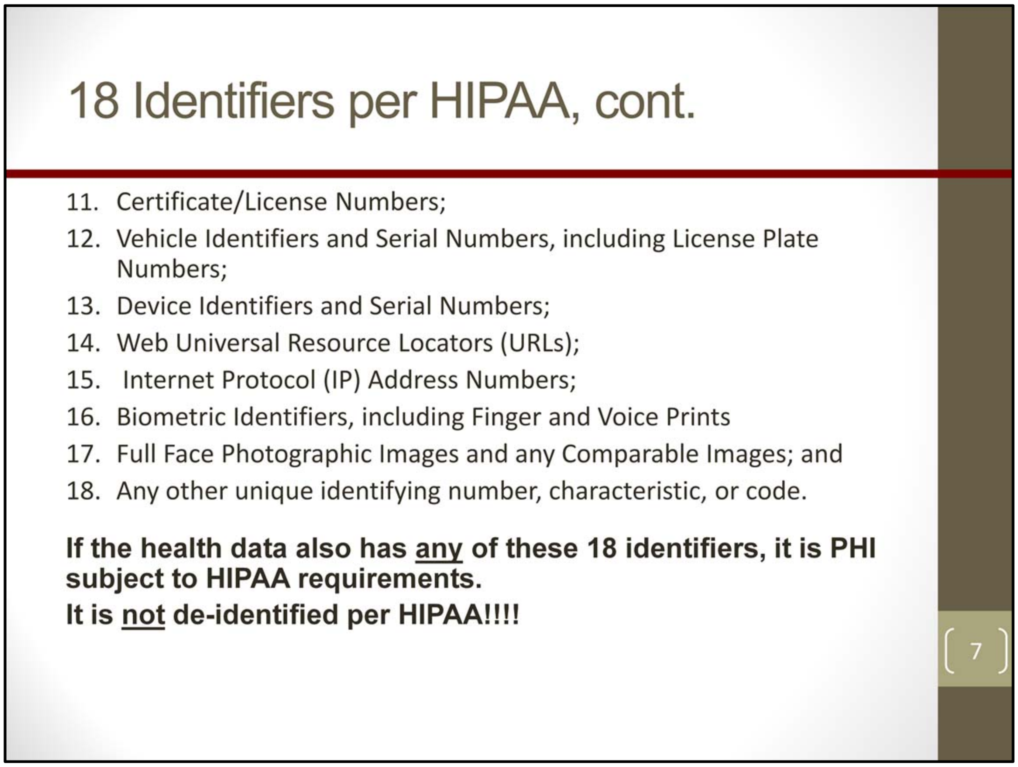


“Individually Identifiable” per HIPAA? 18 Identifiers

1. Names
2. All geographic subdivisions smaller than a State
3. All elements of dates (except year) directly related to an individual, including birth/death, admission/discharge, service dates
4. Telephone Numbers
5. Fax Numbers
6. Electronic Mail Addresses
7. Social Security Numbers
8. Medical Record Numbers
9. Health Plan Beneficiary Numbers

Now that we’ve got the “covered entity” and “health information” parts defined, what constitutes identifiable? More than one might initially think.

These are 18 identifiers set forth by HIPAA. Some categories are obvious such as name, address and identifiers unique to the individuals; however, they also include identifiers that can be cross-references, for example an individual’s medical record or health plan number.



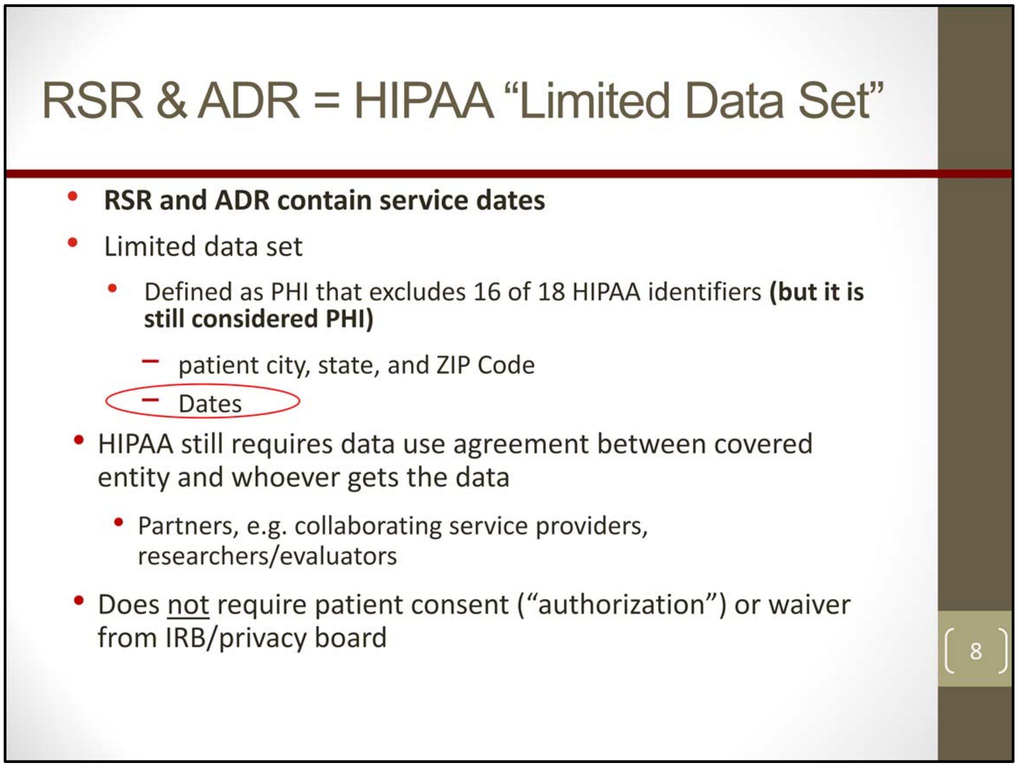
18 Identifiers per HIPAA, cont.

11. Certificate/License Numbers;
12. Vehicle Identifiers and Serial Numbers, including License Plate Numbers;
13. Device Identifiers and Serial Numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) Address Numbers;
16. Biometric Identifiers, including Finger and Voice Prints
17. Full Face Photographic Images and any Comparable Images; and
18. Any other unique identifying number, characteristic, or code.

If the health data also has <u>any</u> of these 18 identifiers, it is PHI subject to HIPAA requirements.

It is <u>not</u> de-identified per HIPAA!!!!

As you see the list continues. We will provide a link at the end of the broadcast where you can access this detail for easy reference later on.



RSR & ADR = HIPAA "Limited Data Set"

- **RSR and ADR contain service dates**
- Limited data set
  - Defined as PHI that excludes 16 of 18 HIPAA identifiers **(but it is still considered PHI)**
    - patient city, state, and ZIP Code
    - Dates
- HIPAA still requires data use agreement between covered entity and whoever gets the data
  - Partners, e.g. collaborating service providers, researchers/evaluators
- Does not require patient consent ("authorization") or waiver from IRB/privacy board

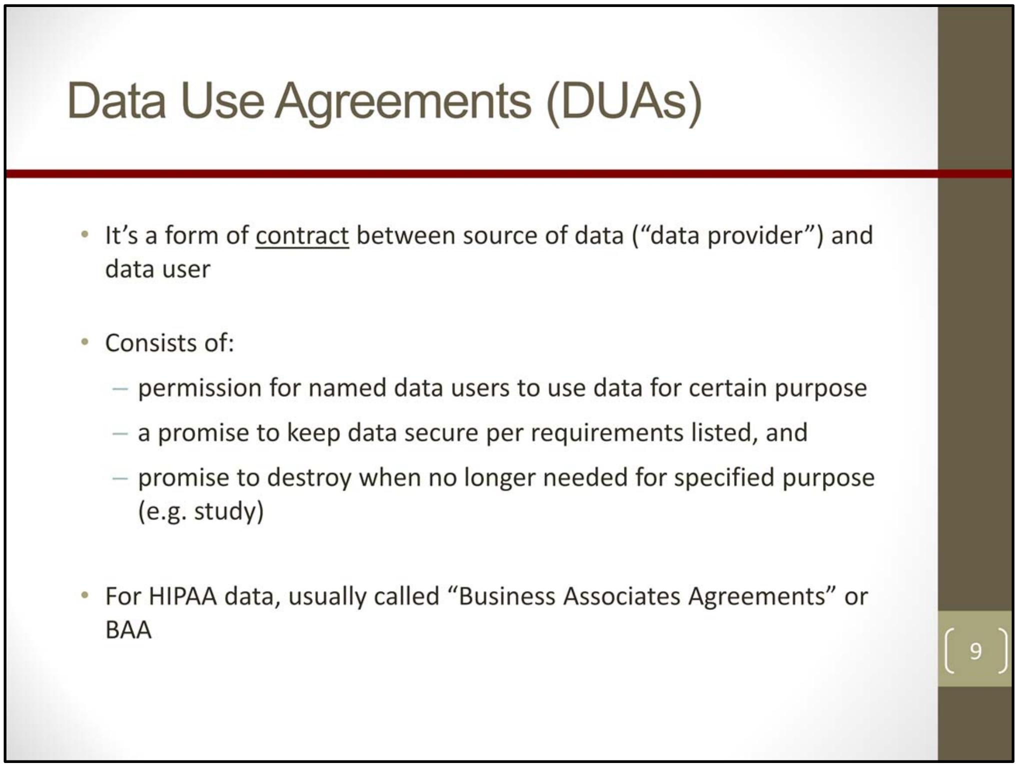
8

As we mentioned a moment ago. Even after the conforming RSR and ADR data sets are created, and the direct identifiers have been removed (such as name and birthdate), there are still identifiers in the data set. These identifiers are the service dates. This means the data set in not fully de-identified. Instead, it is considered a HIPAA "Limited Data Set."

We point this out so you will that you not treat your RSR and ADR conforming data files as though the are de-identified data. Until the service dates are masked or removed, these data are not fully de-identified.

Grantees may decide share their conforming RSR or ADR data with other collaborating service providers to better coordinate services in the community, or with researchers or evaluators to assist with data analysis. So, it is important to remember that before sharing your conforming RSR or ADR data files, you still need to be sure data use agreements are in place.

However, because it is a HIPAA limited data set, patient consent is not required prior to sharing your conforming RSR or ADR data sets.



Data Use Agreements (DUAs)

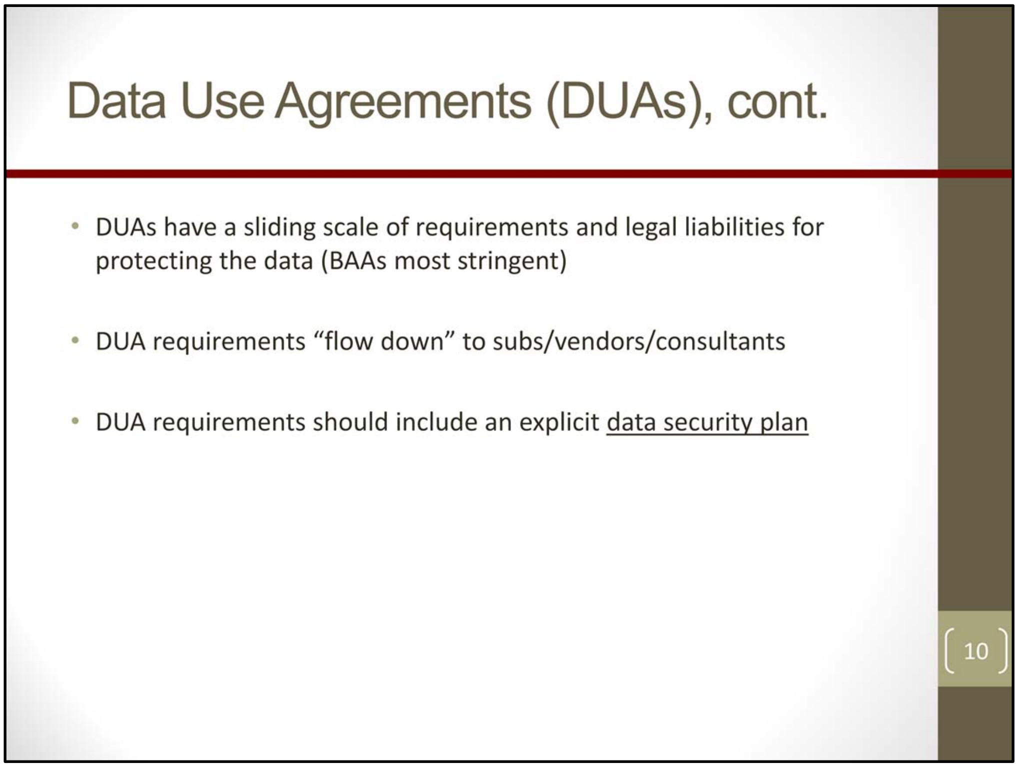
- It’s a form of contract between source of data (“data provider”) and data user
- Consists of:
  - permission for named data users to use data for certain purpose
  - a promise to keep data secure per requirements listed, and
  - promise to destroy when no longer needed for specified purpose (e.g. study)
- For HIPAA data, usually called “Business Associates Agreements” or BAA

9

I just brought up DUA’s, so lets take a deeper dive on just what a DUA actually is. Basically, it’s a contract that lays out a binding agreement between someone providing data - and someone receiving data. DUAs have three main parts:

- identifying the specific uses of the data,
- the practices and standards for maintaining the data, and
- the date by which data will be returned or destroyed.

Under HIPAA, such agreements are often termed “Business Associates Agreements.”



Data Use Agreements (DUAs), cont.

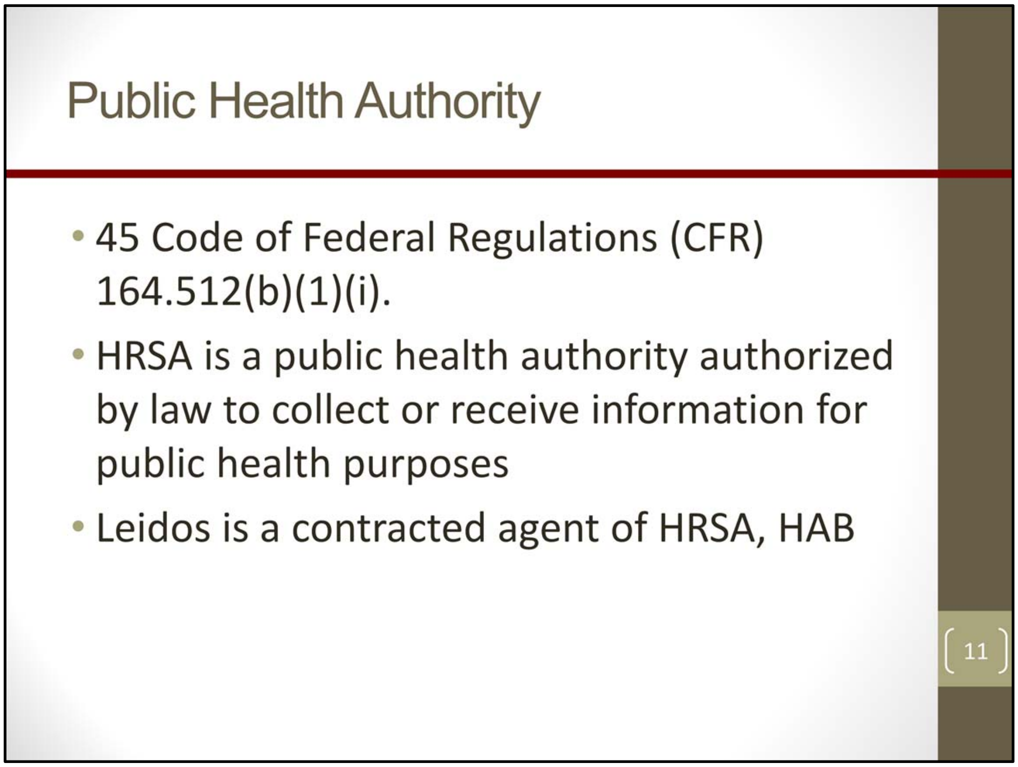
- DUAs have a sliding scale of requirements and legal liabilities for protecting the data (BAAs most stringent)
- DUA requirements “flow down” to subs/vendors/consultants
- DUA requirements should include an explicit data security plan

Some other important things to keep in mind about DUAs :

- The requirements and legal liabilities are not fixed, but can be a “sliding scale” based upon the risk assessment by the entity providing the data.

- Anytime there is subcontractor under the entity that received the data through a DUA …the requirements of that DUA flow down to the sub contractor. That is to say, they are bound by the same requirements as their prime contractor that signed the DUA.

- DUAs should included a data security plan that lays out the specific requirements to protect the data.



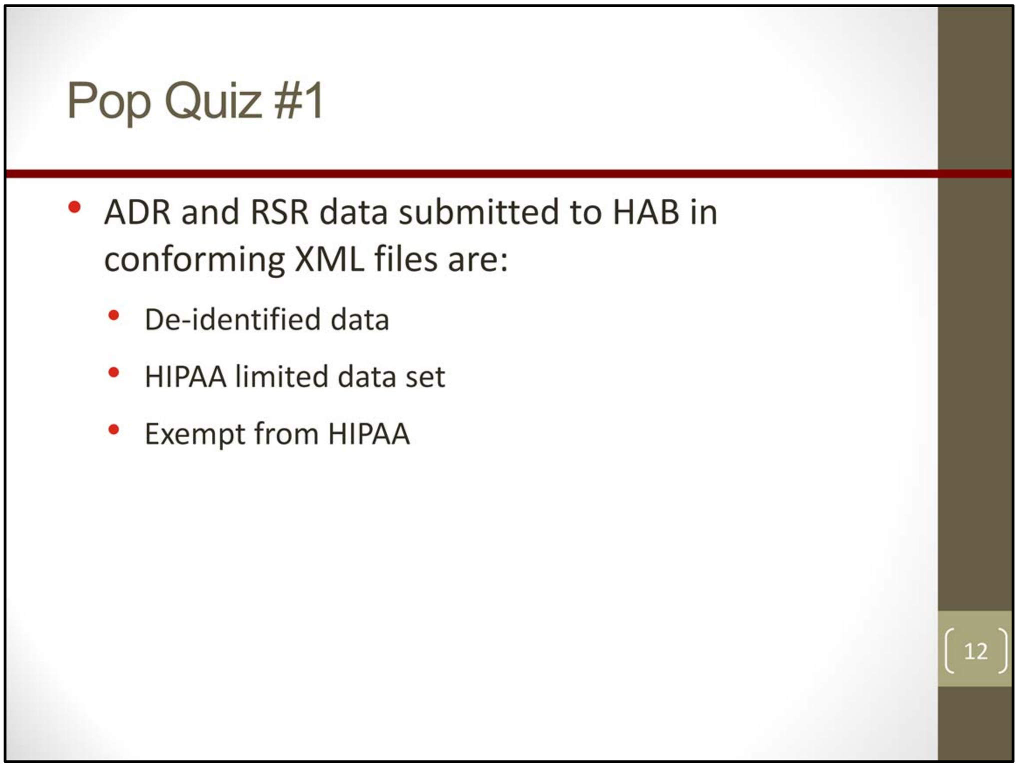
Public Health Authority

- 45 Code of Federal Regulations (CFR) 164.512(b)(1)(i).
- HRSA is a public health authority authorized by law to collect or receive information for public health purposes
- Leidos is a contracted agent of HRSA, HAB

11

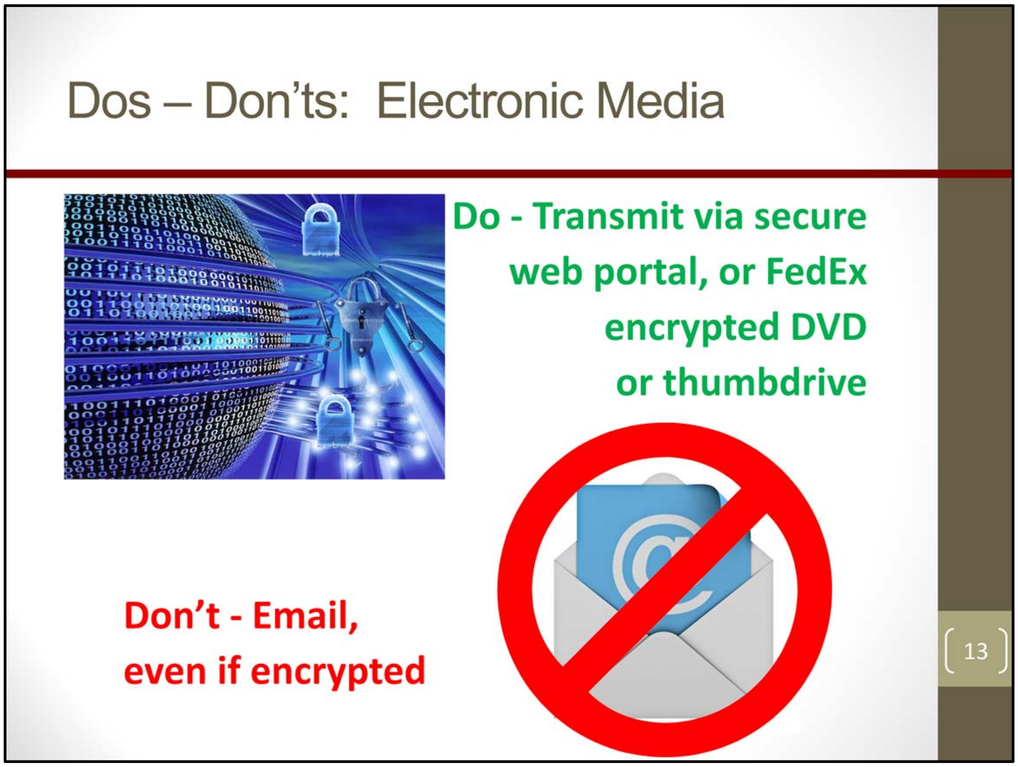
So with all this talk of DUAs, how is it possible for grantees to send data to HAB without a DUA? The privacy rule in the Code of Federal Regulations permits covered entities to disclose PHI to authorized public health authorities for the purposes of preventing or controlling disease, injury, or disability. This includes reporting of a disease or injury and conducting public health surveillance, investigations, or interventions.

Leidos (the firm to which RSR and ADR conforming data files are uploaded) is a contracted agent of HRSA, and so can receive the such data on HAB’s behalf.



Pop Quiz #1

- ADR and RSR data submitted to HAB in conforming XML files are:
  - De-identified data
  - HIPAA limited data set
  - Exempt from HIPAA



Dos – Don’ts: Electronic Media

Do - Transmit via secure web portal, or FedEx encrypted DVD or thumbdrive

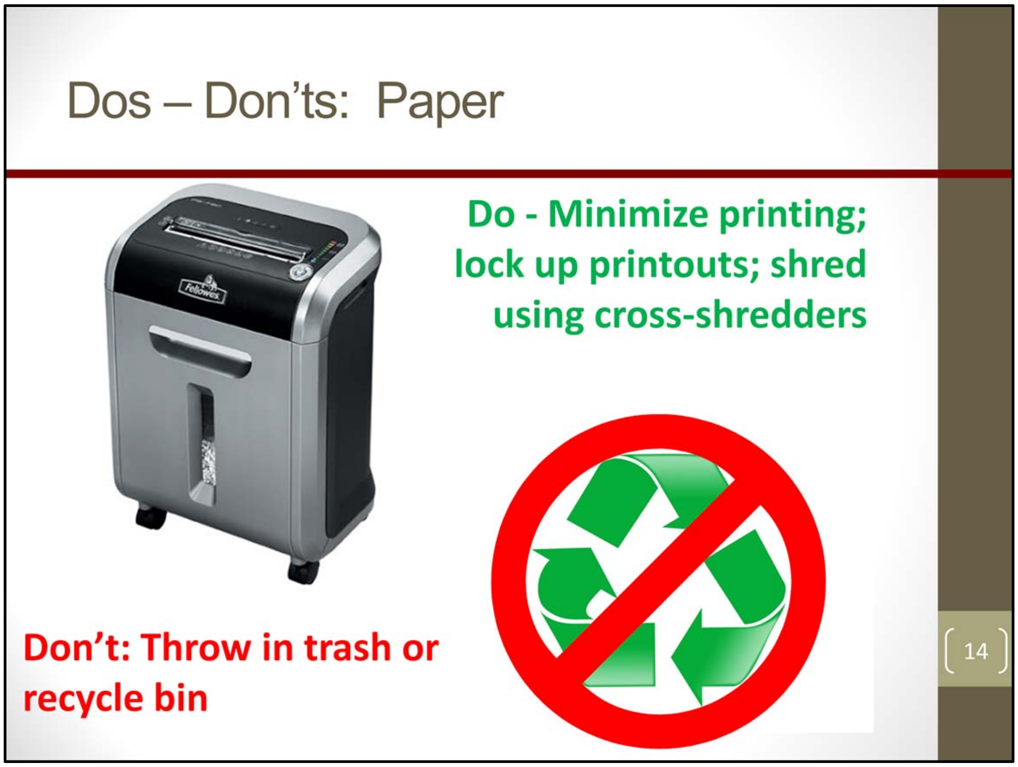
Don’t - Email, even if encrypted

13

Next I’ll review some overall “do’” and “don’ts” when it comes to keeping your data secure.

First, if you need to transmit your data electronically, only use secure means to do so. Data should only be transferred via the secure method specified in the DUA. This may include secure web portals, encrypted DVDs or thumb drives.

Never email files, even if you have encrypted them. Email is not secure. Messages and files sent by email can be intercepted and read by others. Email is also prone to human error, such as forgetting to encrypt files or sending to the wrong person.

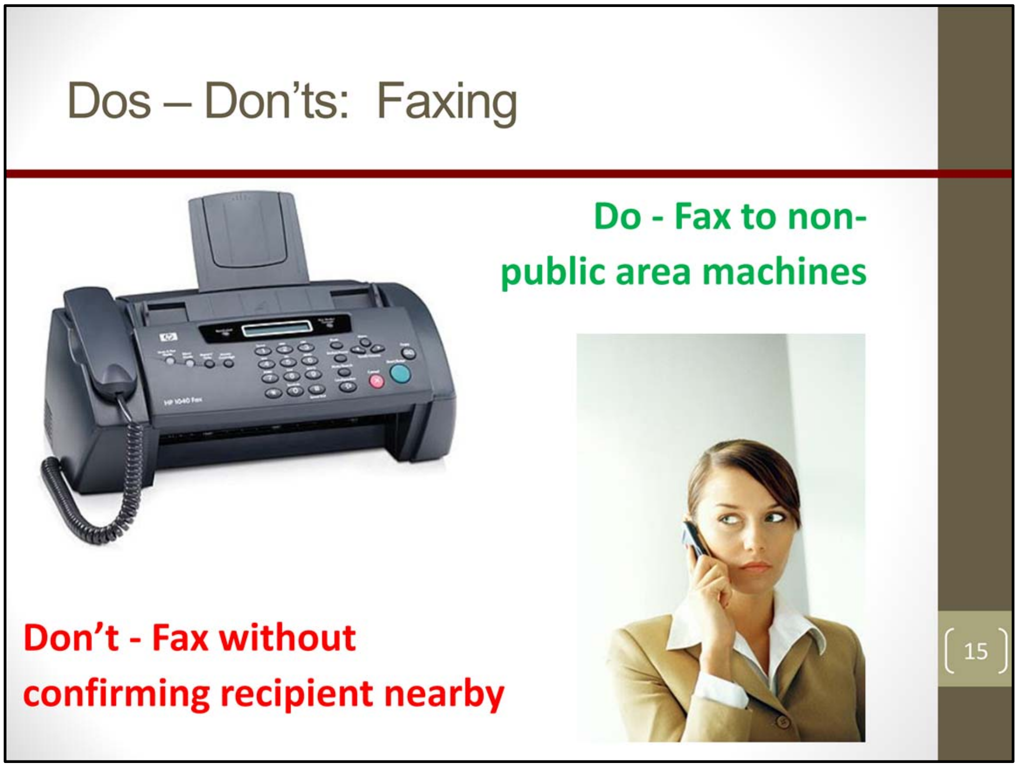


Dos – Don’ts: Paper

Do - Minimize printing; lock up printouts; shred using cross-shredders

Don’t: Throw in trash or recycle bin

If you must use create printouts of PHI, minimize it to the extent possible. Keep printouts secured in locked cabinets - and always shred it (using a cross=-shredder) when you are through using the printouts. Never throw printouts with PHI in the trash or recycle bin.



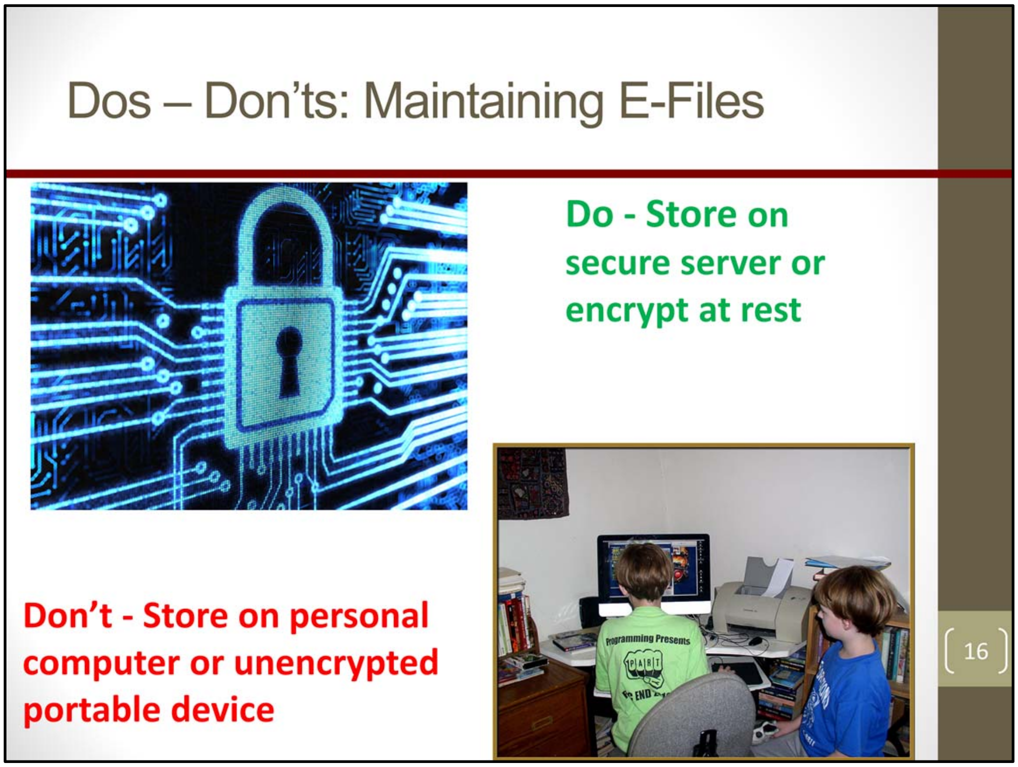
Dos – Don’ts: Faxing

Do - Fax to non-public area machines

Don’t - Fax without confirming recipient nearby

15

When faxing data be sure you are not faxing to a machine located in a public area – and always confirm receipt by the intended recipient.

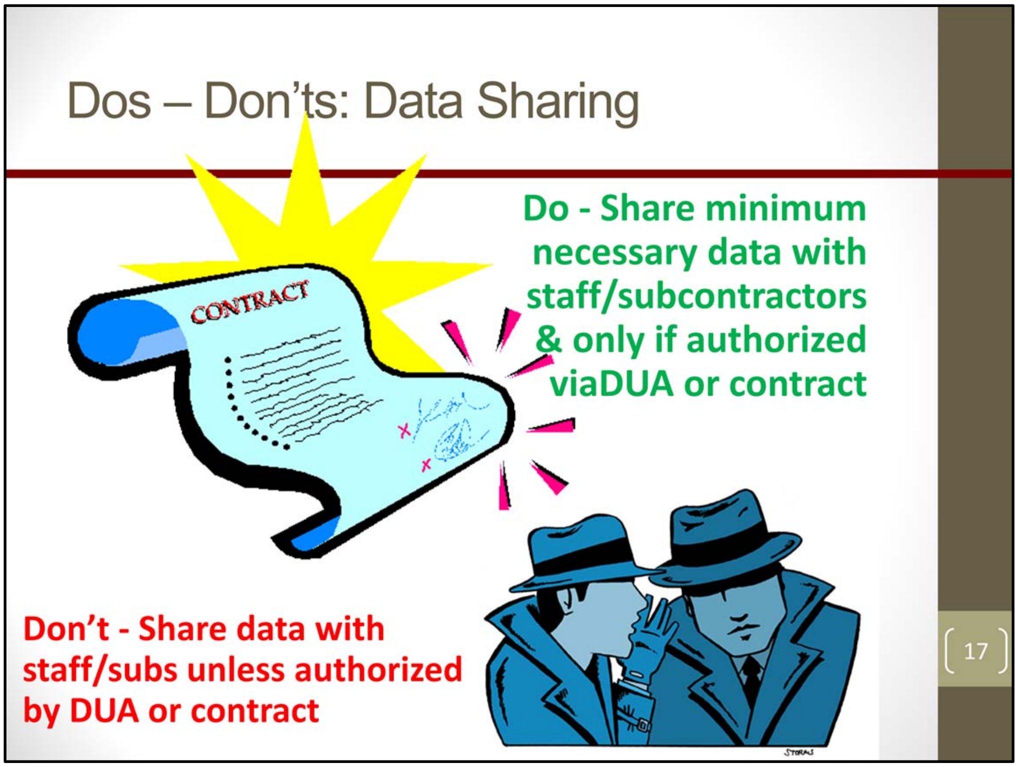


Dos – Don’ts: Maintaining E-Files

Do - Store on secure server or encrypt at rest

Don’t - Store on personal computer or unencrypted portable device

Confirm with your IT security staff that you are using secure servers. If you are not sure your servers are secure, encrypt the files when you are not actively working on them. This is called “encryption at rest.” Do not keep PHI on a personal computer or unencrypted portable device, such as a laptop, tablet or smartphone.



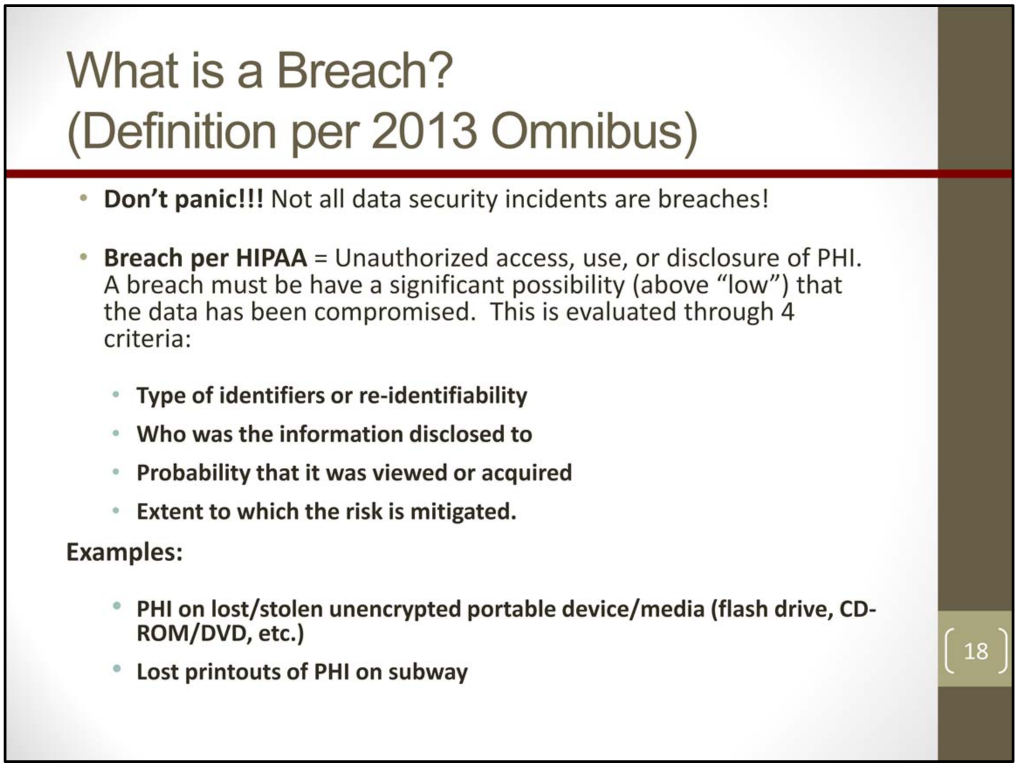
Dos – Don'ts: Data Sharing

Do - Share minimum necessary data with staff/subcontractors & only if authorized viaDUA or contract

Don't - Share data with staff/subs unless authorized by DUA or contract

17

When sharing data, be sure you have a DUA in place clearly delineating the terms of data use and protection – and only ever share the absolute minimum to meet the intended needs. This is one of those cases where less is more. Do not share data with parties you do not have a DUA or BAA with. Verbal agreements are not appropriate for securing PHI. Even the best intentioned parties can slip on data security if the goals and rules of the road are not clearly laid out. If you aren't sure someone is authorized to receive HIPAA data, then ask first.



What is a Breach? (Definition per 2013 Omnibus)

- **Don't panic!!!** Not all data security incidents are breaches!
- **Breach per HIPAA** = Unauthorized access, use, or disclosure of PHI. A breach must be have a significant possibility (above "low") that the data has been compromised. This is evaluated through 4 criteria:
  - **Type of identifiers or re-identifiability**
  - **Who was the information disclosed to**
  - **Probability that it was viewed or acquired**
  - **Extent to which the risk is mitigated.**

Examples:

- **PHI on lost/stolen unencrypted portable device/media (flash drive, CD-ROM/DVD, etc.)**
- **Lost printouts of PHI on subway**

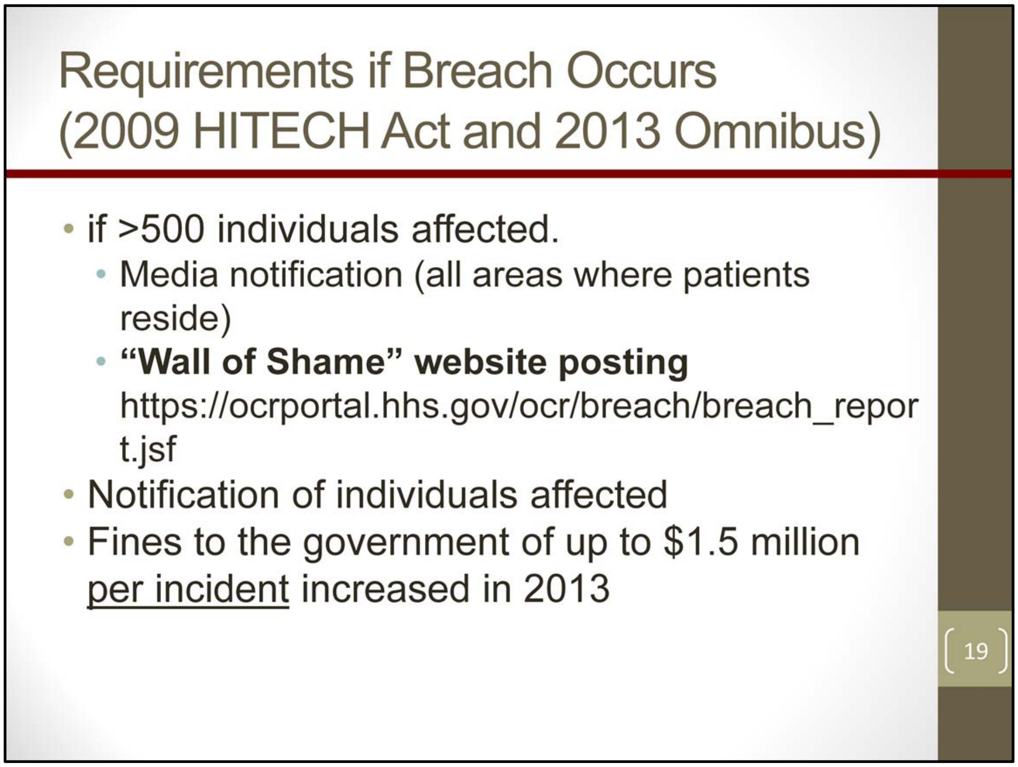
18

A little while ago we used the word "breaches." For those who know what those are and felt a wave of adrenaline – don't panic!

Not all data security incidents rise to the level of a "breach." There are four criteria that are applied to determine if an actual breach occurred and the data were compromised. These criteria focus on four questions:

- What type of identifiers were in the file and what is the level of re-identifiability?
- To whom was the information disclosed?
- What is the probability that the data were actually viewed of acquired?
- Who fully was the risk mitigated?

Examples of actual breaches include:
- PHI on lost or stolen unencrypted portable devices and media such as flash drives and CD-ROMs
- Lost printouts of PHI left on a subway, for those who don't remember this was in the news a few years back.



Requirements if Breach Occurs (2009 HITECH Act and 2013 Omnibus)

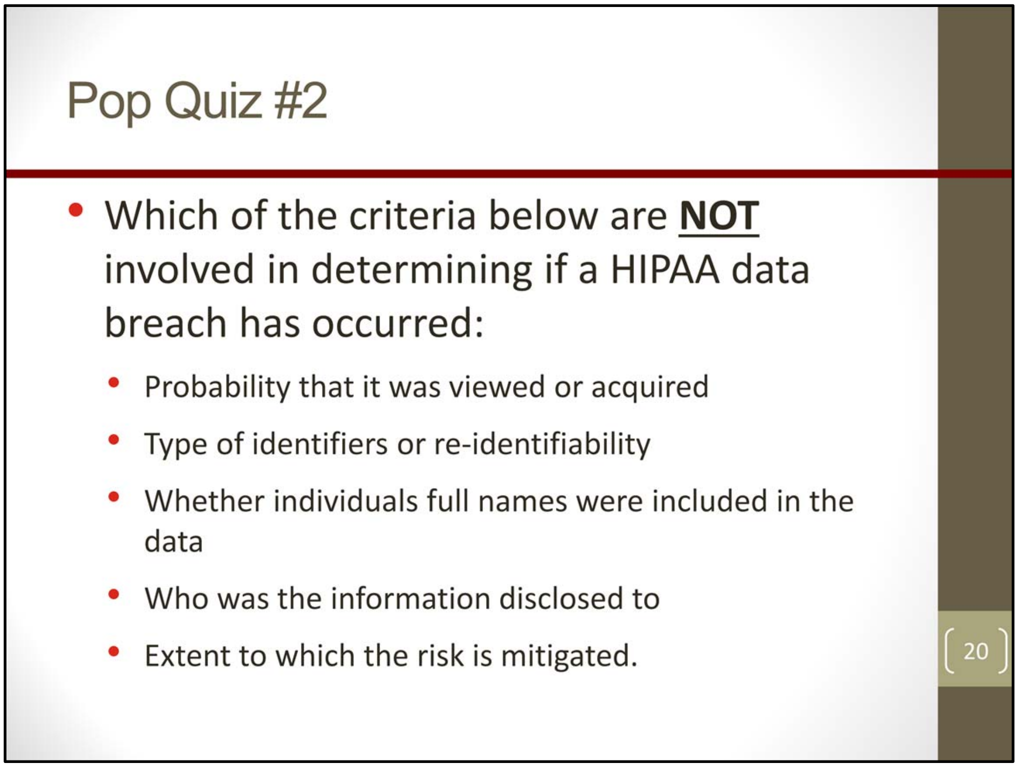
- if >500 individuals affected.
  - Media notification (all areas where patients reside)
  - **"Wall of Shame" website posting** https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Notification of individuals affected
- Fines to the government of up to $1.5 million <u>per incident</u> increased in 2013

If there is an actual breach. The penalties have gotten quite severe.

If the data of more than 500 people were affected then the media in area of the affected individuals must be notified. "Affected individuals" refers to the people whose data were exposed. Also, if the data of more than 500 people were affected the the incident is posted on the "Wall of Shame." You can go take a look at the postings if want to get the shivers.

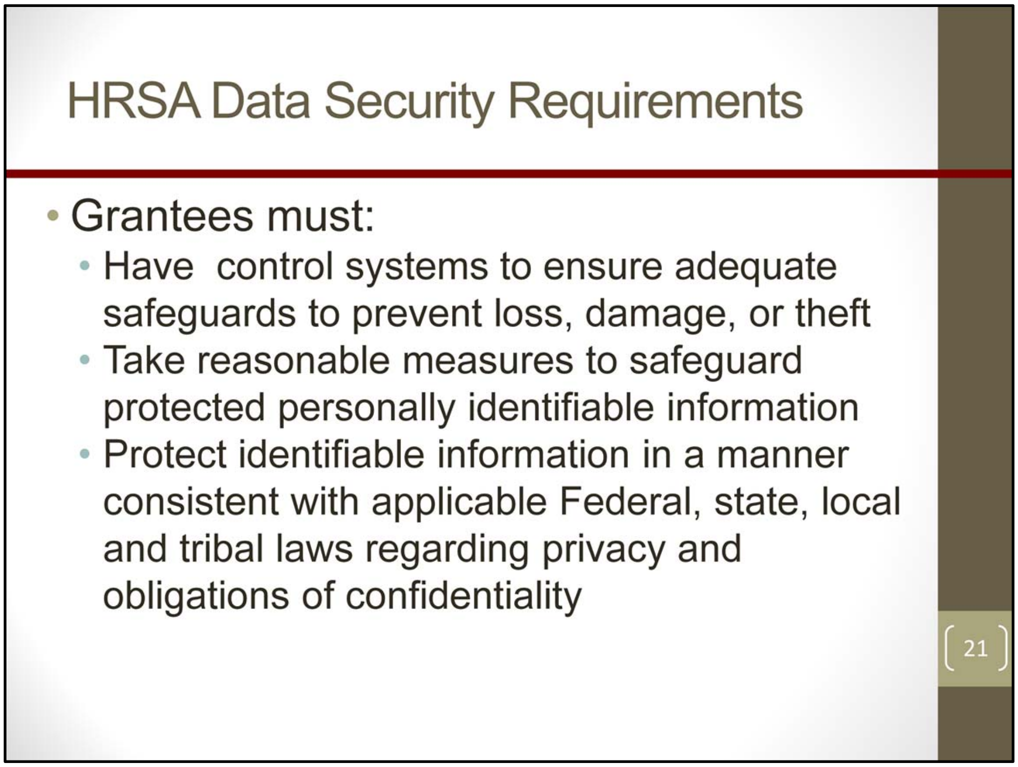
The individuals whose data was compromised must be individually notified.

There can be a fine for the organization of up to 1.5 million dollars for the incident.



Pop Quiz #2

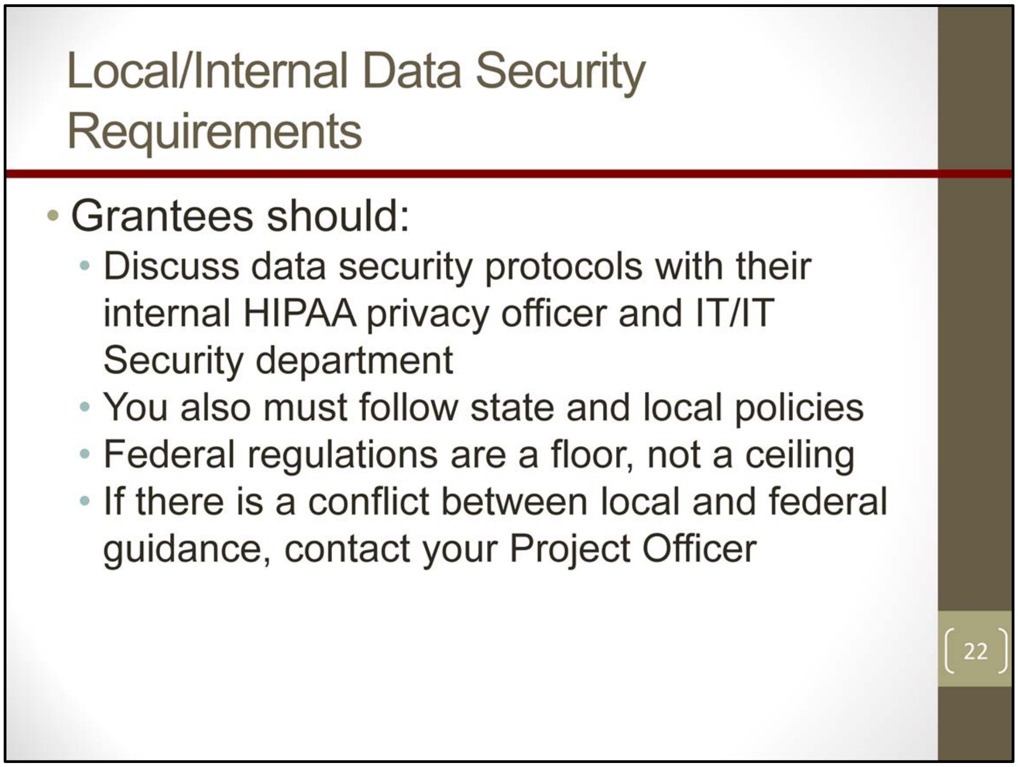
- Which of the criteria below are **NOT** involved in determining if a HIPAA data breach has occurred:
  - Probability that it was viewed or acquired
  - Type of identifiers or re-identifiability
  - Whether individuals full names were included in the data
  - Who was the information disclosed to
  - Extent to which the risk is mitigated.



HRSA Data Security Requirements

- Grantees must:
  - Have control systems to ensure adequate safeguards to prevent loss, damage, or theft
  - Take reasonable measures to safeguard protected personally identifiable information
  - Protect identifiable information in a manner consistent with applicable Federal, state, local and tribal laws regarding privacy and obligations of confidentiality

HRSA has grants requirements in place to ensure that grantees are held accountable for data security. Grant regulations, for all grantees, state that they must have for their equipment, a “control system…to ensure adequate safeguards to prevent loss, damage, or theft.” And, for internal controls, the grant regulations state that grantees must “take reasonable measures to safeguard protected personally identifiable information and other information the HHS awarding agency or pass-through entity designates as sensitive …consistent with applicable Federal, state, local and tribal laws regarding privacy and obligations of confidentiality.” If a grantee is not compliant with these expectations, then HRSA has the discretion to place a condition on the grant recipient and also monitor for any needed corrective action.

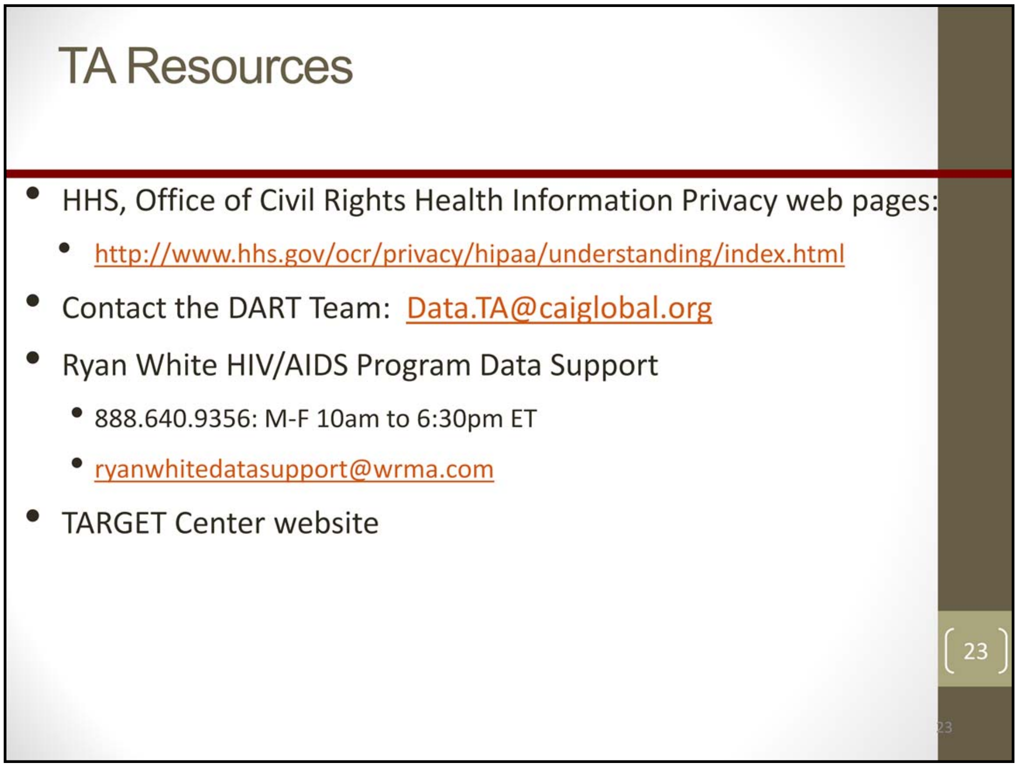


Local/Internal Data Security Requirements

- Grantees should:
  - Discuss data security protocols with their internal HIPAA privacy officer and IT/IT Security department
  - You also must follow state and local policies
  - Federal regulations are a floor, not a ceiling
  - If there is a conflict between local and federal guidance, contact your Project Officer

Most grantees are covered entities and, as such, have their own internal data security protocols. We encourage you to confer with your internal HIPAA and data security staff. There may also be additional state regulations regarding PHI, particularly as it relates to HIV data. Federal data security regulations are a floor, not a ceiling.

If any of your internal requirements or local regulations seem to be in conflict with federal guidances, please reach out your project officer to discuss.



TA Resources

- HHS, Office of Civil Rights Health Information Privacy web pages:
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- Contact the DART Team: Data.TA@caiglobal.org
- Ryan White HIV/AIDS Program Data Support
  - 888.640.9356: M-F 10am to 6:30pm ET
  - ryanwhitedatasupport@wrma.com
- TARGET Center website

23

Here are a list resources available to you:

The HHS, Office of Civil Rights Health Information Privacy web pages provides in-depth detail regarding HIPAA rules, training materials and enforcement activities.

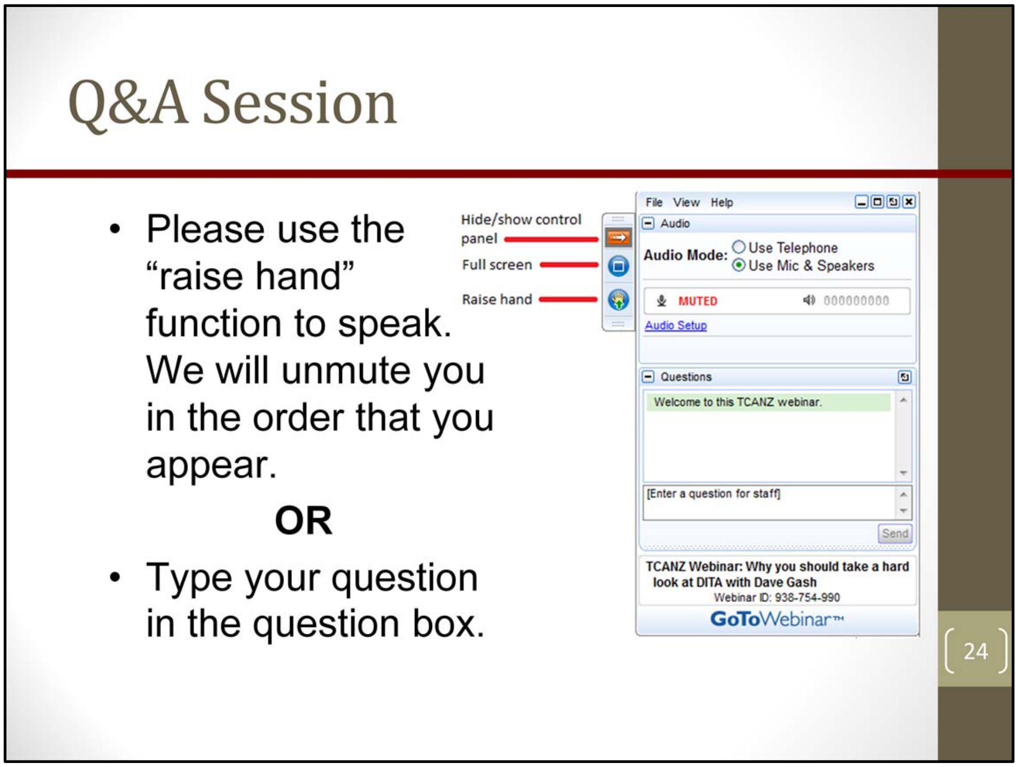
The DART Team addresses questions for those needing significant assistance to meet data reporting requirements, such as helping grantees who do not know what to do or where to start; Determining if grantee systems currently collect required data; Assisting grantees in extracting data from their systems and reporting it using the required XML schema; Connecting grantees to other grantees that use the same data system, as well as helping grantees determine data security needs.

DART also deal with data quality issues, as well as providing TA on the encrypted Unique Client Identifier (eUCI) Application.

Data Support addresses RSR-related content and submission questions. Topics include: Interpretation of the RSR Instruction Manual and HAB’s reporting requirements; Allowable responses to data elements of the RSR Grantee Report and client-level data file; Policy questions related to the data reporting requirements and data-related validation questions.

TARGET Center - has a wealth of materials about of stages of the data collection, management and reporting process.

Now I’ll turn this back over to Ellie to take your question.



Q&A Session

- Please use the "raise hand" function to speak. We will unmute you in the order that you appear.

OR

- Type your question in the question box.

Welcome to this TCANZ webinar.

TCANZ Webinar: Why you should take a hard look at DITA with Dave Gash
Webinar ID: 938-754-990

Thanks Michael. Before we go to the Q&A session, I would like to remind you that a brief, three-question evaluation will appear on your screen as you exit, to help us understand how we did and what other information you would have liked included on this webcast. We appreciate your feedback very much, and use this information to plan future webcasts.

[Advance slide to "TA Resources" during Q&A period].

We will now take questions. As a reminder, you can send us questions using the "Question" function on your control panel on the right hand side of the screen. You can also ask questions directly "live." You can do this by clicking the raise hand button (on your control panel). If you are using a headset with a microphone, my colleague, Titi, will conference you in; or, you can click the telephone button and you will see a dial in number and code. We hope you consider asking questions "live", we really like hearing voices other than our own.

We do want to get all of your questions answered, and we do not usually run over an hour. If you have submitted your question in the question box and we cannot respond to your question today, we will contact you to follow up. We often need to explore your question in order to give you the most appropriate answer.

As you exit this webcast, please complete the evaluation question that appears on your screen. This will help us understand how we did and what other information you would have liked included on this webcast. We appreciate your feedback very much, and use this information to plan future webcasts. Thank you for joining us today!