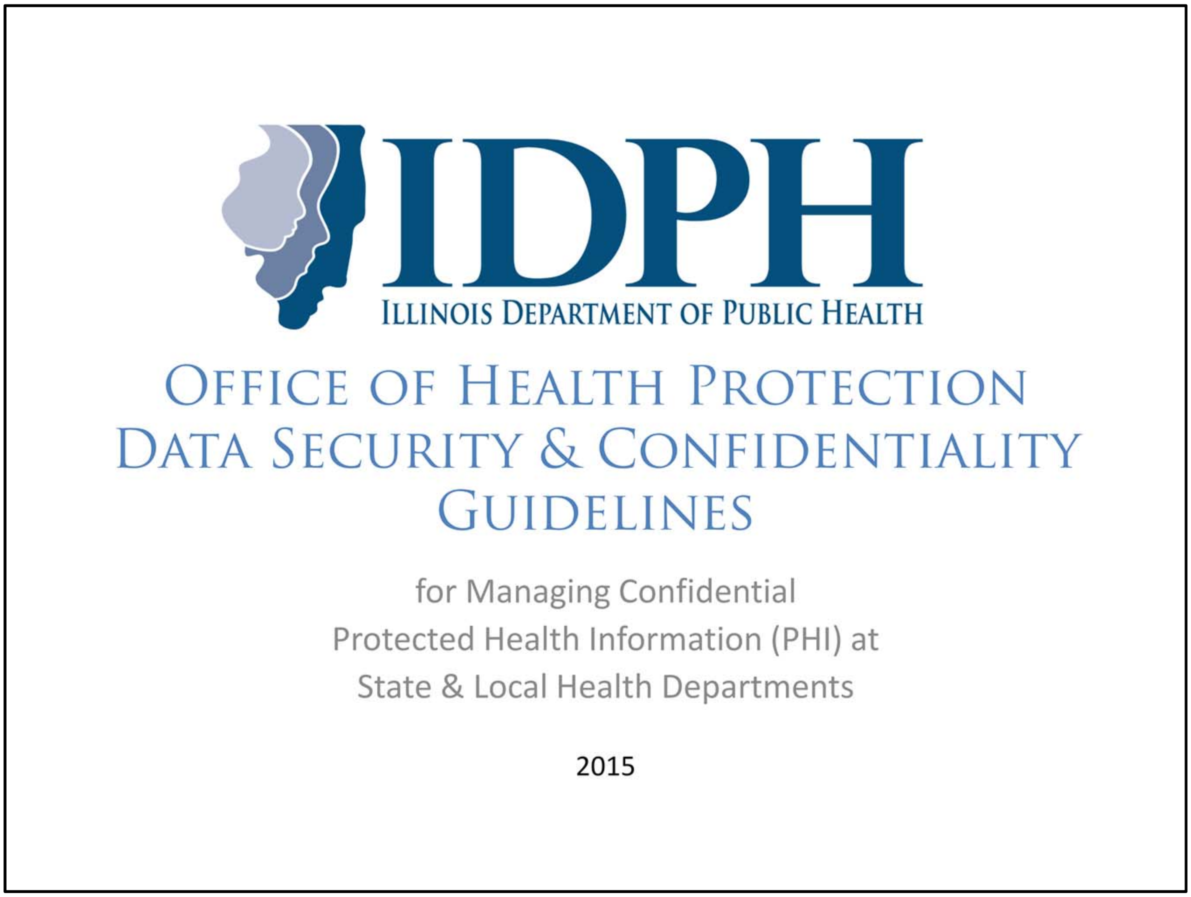


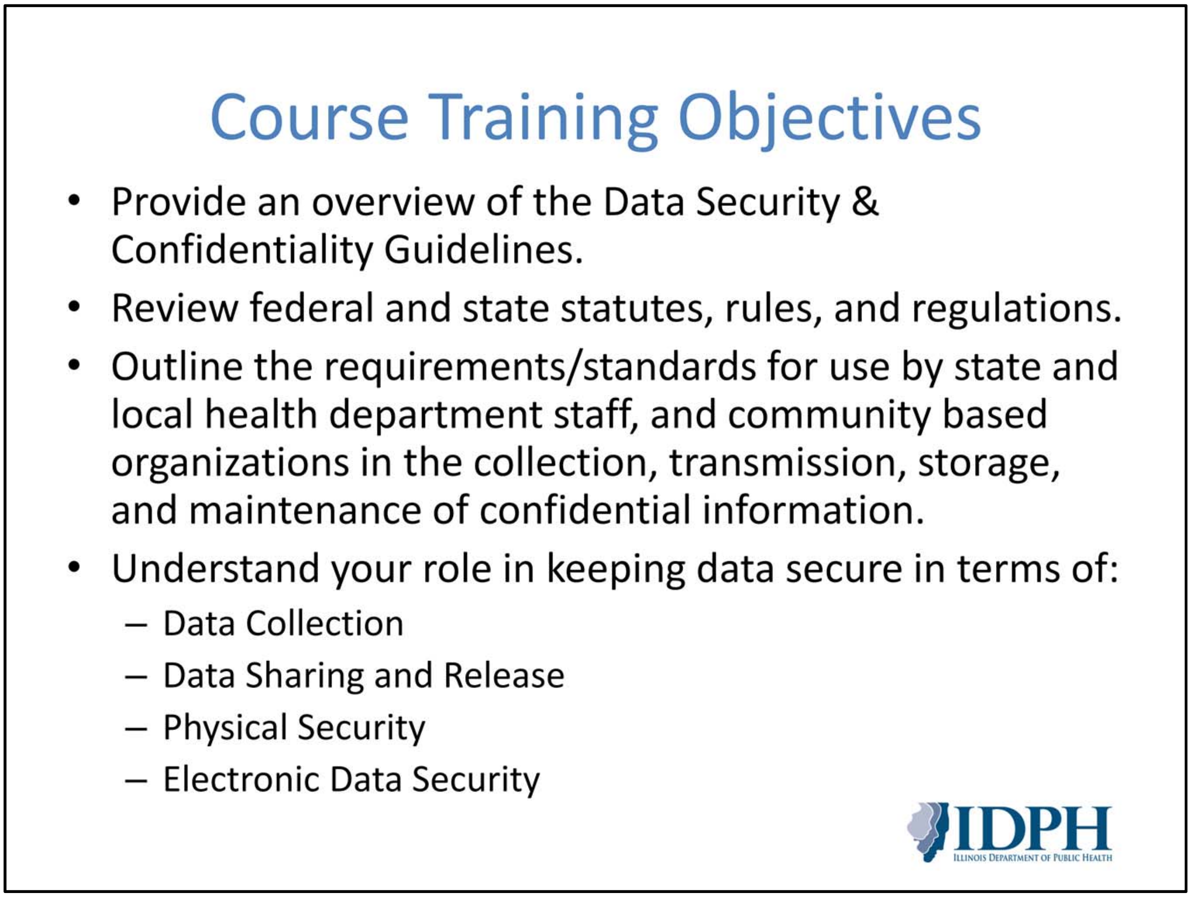
IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

OFFICE OF HEALTH PROTECTION DATA SECURITY & CONFIDENTIALITY GUIDELINES

for Managing Confidential
Protected Health Information (PHI) at
State & Local Health Departments

2015

Hello and thank you for taking part in the Illinois Department of Public Health Office of Health Protection Data Security and Confidentiality Training.



Course Training Objectives

- Provide an overview of the Data Security & Confidentiality Guidelines.
- Review federal and state statutes, rules, and regulations.
- Outline the requirements/standards for use by state and local health department staff, and community based organizations in the collection, transmission, storage, and maintenance of confidential information.
- Understand your role in keeping data secure in terms of:
  - Data Collection
  - Data Sharing and Release
  - Physical Security
  - Electronic Data Security

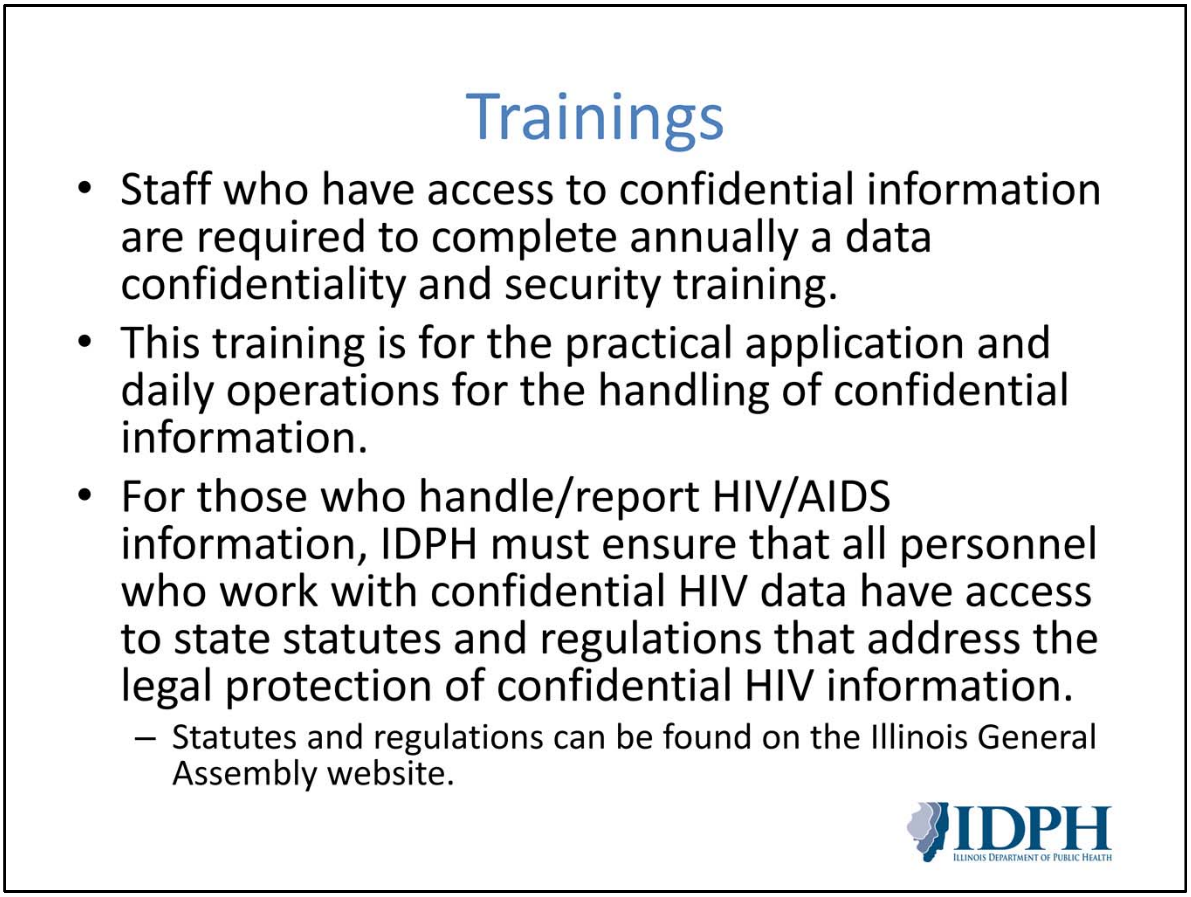
IDPH
Illinois Department of Public Health

The objectives for this training are to:
Provide an overview of the Data Security and Confidentiality Guidelines developed by the Illinois Department of Public Health Office of Health Protection;

Review the federal and state statutes, rules, and regulations; and for those who handle and report HIV/AIDS, address the legal protection of HIV/AIDS information;

Outline the requirements and standards for use by state and local health department staff as well as community based organizations in the collection, transmission, storage, and maintenance of confidential information.

And lastly, help in understanding your role in keeping data secure in terms of data collection, data sharing and release as well as provide examples of physical and electronic data and how to properly secure these various types of data sets.

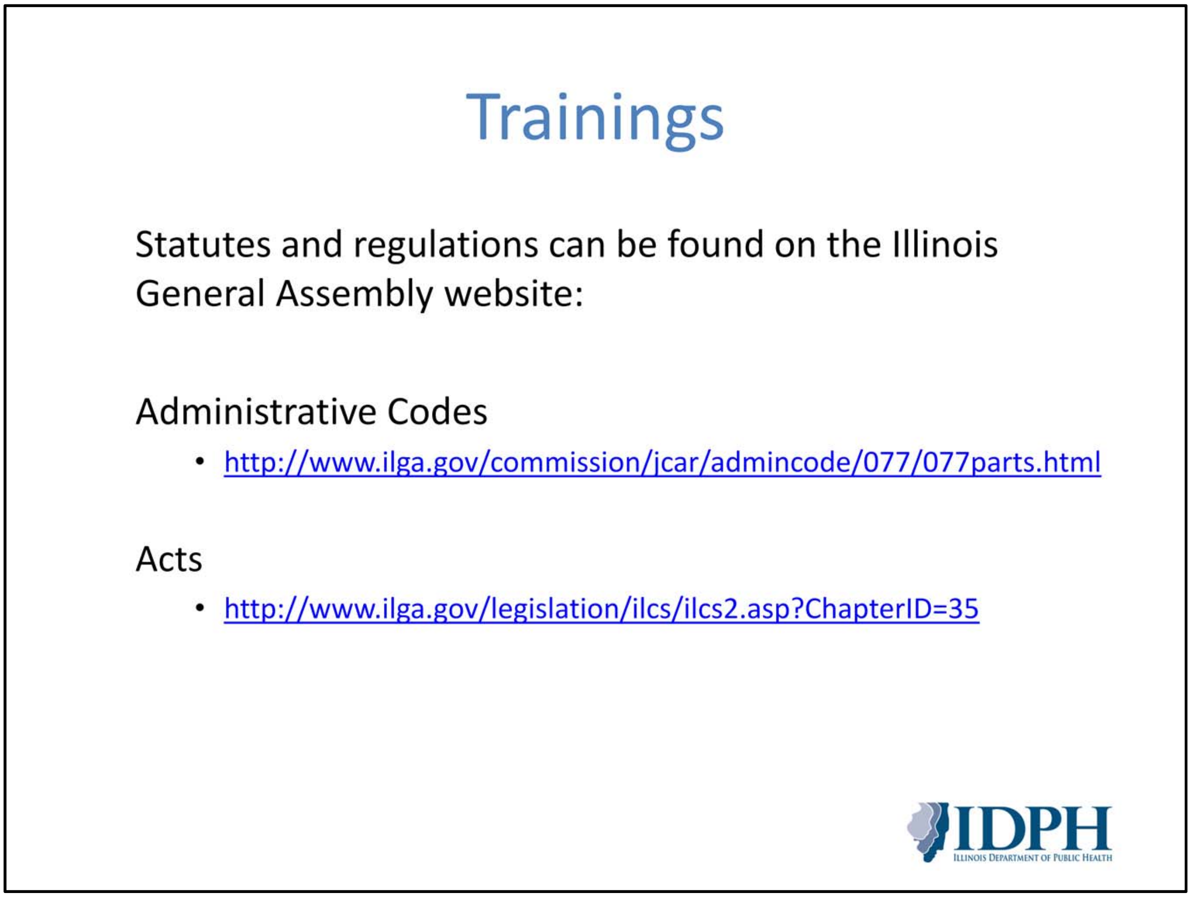


Trainings

- Staff who have access to confidential information are required to complete annually a data confidentiality and security training.
- This training is for the practical application and daily operations for the handling of confidential information.
- For those who handle/report HIV/AIDS information, IDPH must ensure that all personnel who work with confidential HIV data have access to state statutes and regulations that address the legal protection of confidential HIV information.
  - Statutes and regulations can be found on the Illinois General Assembly website.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Annually, staff who have access to confidential information are required to complete a data confidentiality and security training that reviews the practical application and daily operations for the handling of confidential information.



Trainings

Statutes and regulations can be found on the Illinois General Assembly website:

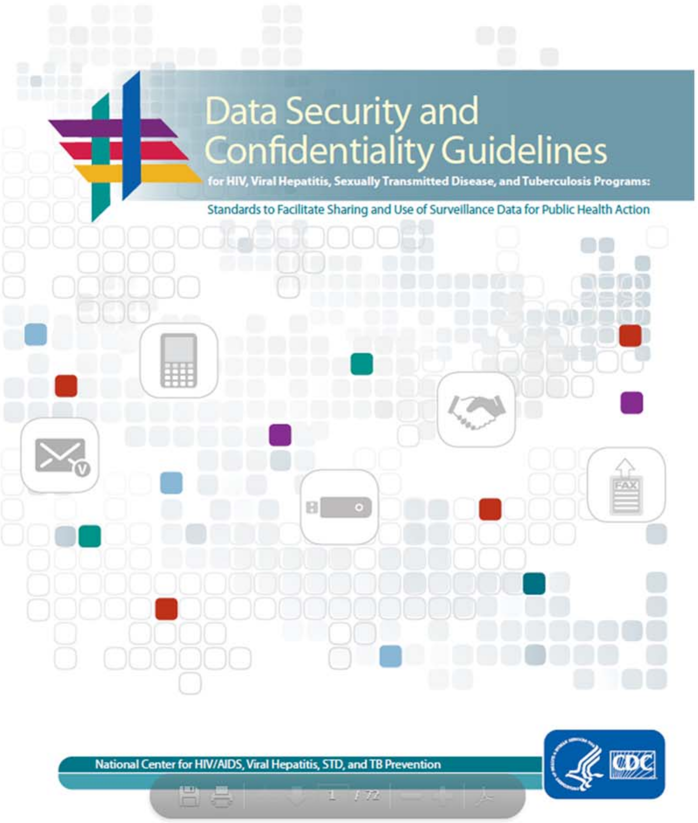
Administrative Codes

- http://www.ilga.gov/commission/jcar/admincode/077/077parts.html

Acts

- http://www.ilga.gov/legislation/ilcs/ilcs2.asp?ChapterID=35

The Illinois Department of Public Health must ensure that all personnel who work with confidential HIV data have access to state statutes and regulations that address the legal protection of confidential HIV information. These statutes and regulations can be found on the Illinois General Assembly website.



Data Security and Confidentiality Guidelines

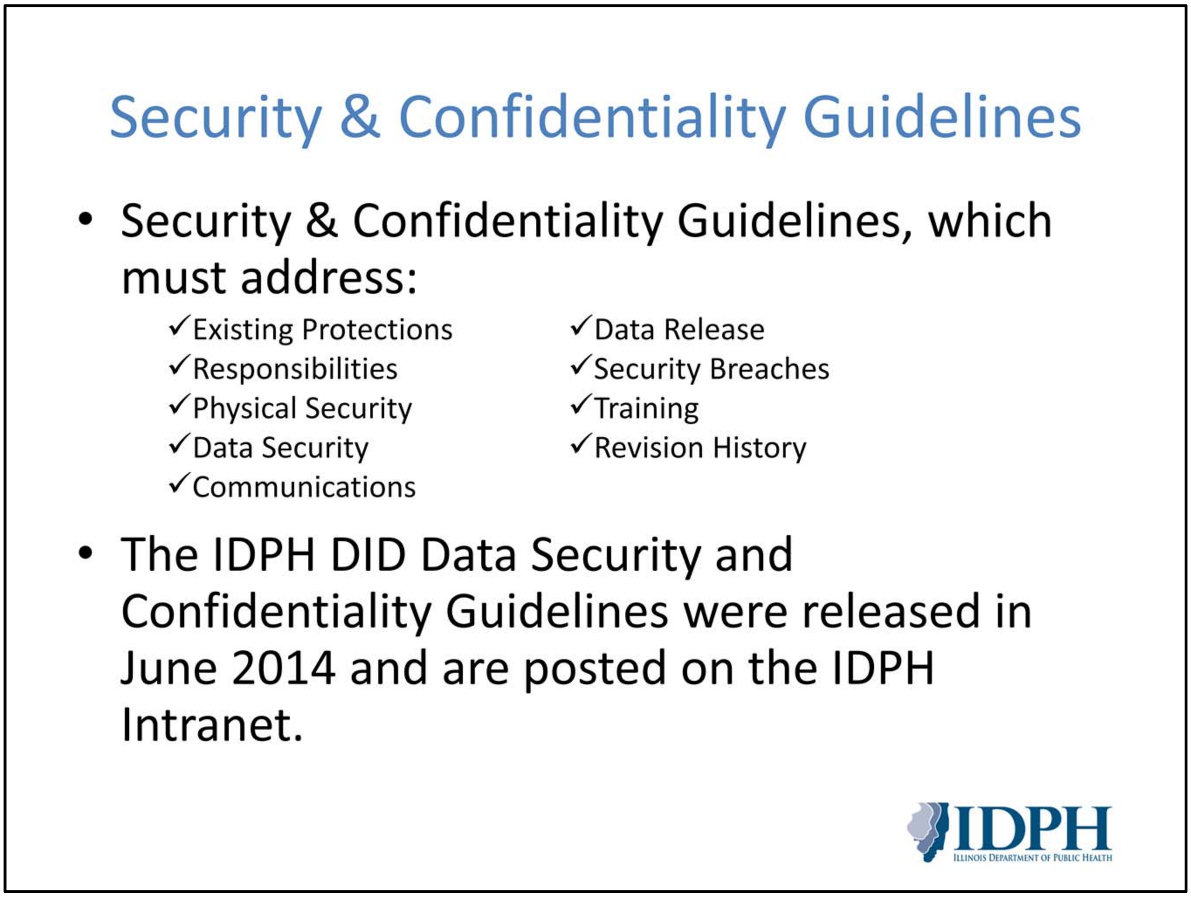
for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs:

Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action

National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention

IDPH
Illinois Department of Public Health

The Centers for Disease Control and Prevention (or CDC) requires that sites funded for viral hepatitis, TB, HIV and STD activities to establish Security and Confidentiality Guidelines.



Security & Confidentiality Guidelines

- Security & Confidentiality Guidelines, which must address:
  - ✓Existing Protections
  - ✓Responsibilities
  - ✓Physical Security
  - ✓Data Security
  - ✓Communications
  - ✓Data Release
  - ✓Security Breaches
  - ✓Training
  - ✓Revision History
- The IDPH DID Data Security and Confidentiality Guidelines were released in June 2014 and are posted on the IDPH Intranet.

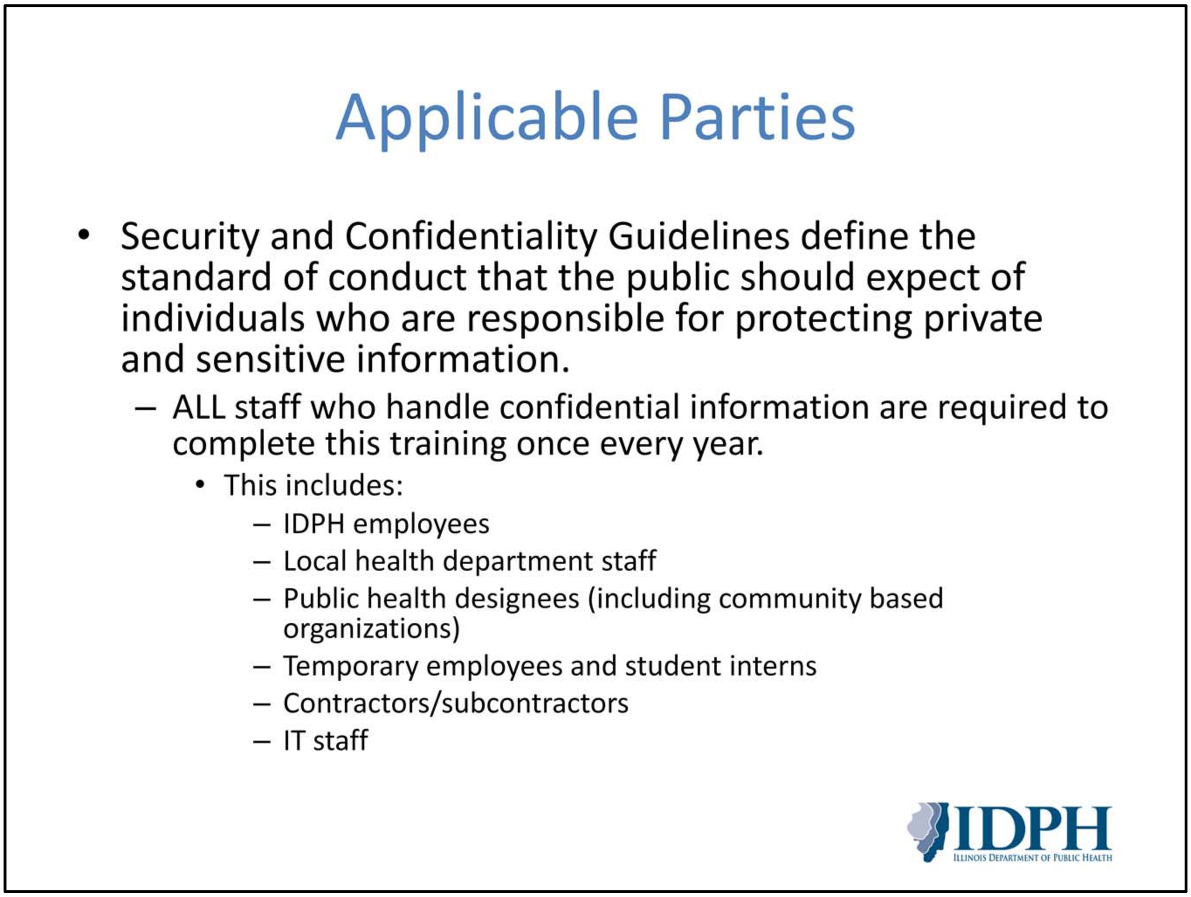
IDPH
Illinois Department of Public Health

Local health departments and community based organizations are encouraged to implement their own local Data Security and Confidentiality Guidelines; however, the minimum security standards outlined in the state guidelines must be in place.

The guidelines must address the following:
Existing Protections, Responsibilities, Physical Security, Data Security, Communications, Data Release, Security Breaches, Training, Revision History

All of these topics will be covered in this training.

Based off of the federal guidelines, as well as existing HIV/AIDS Confidentiality & Security Policy, in place since March 2009, the Illinois Department of Public Health Division of Infectious Diseases Data Security and Confidentiality Guidelines were released in June 2014 and can be found on the IDPH Intranet.



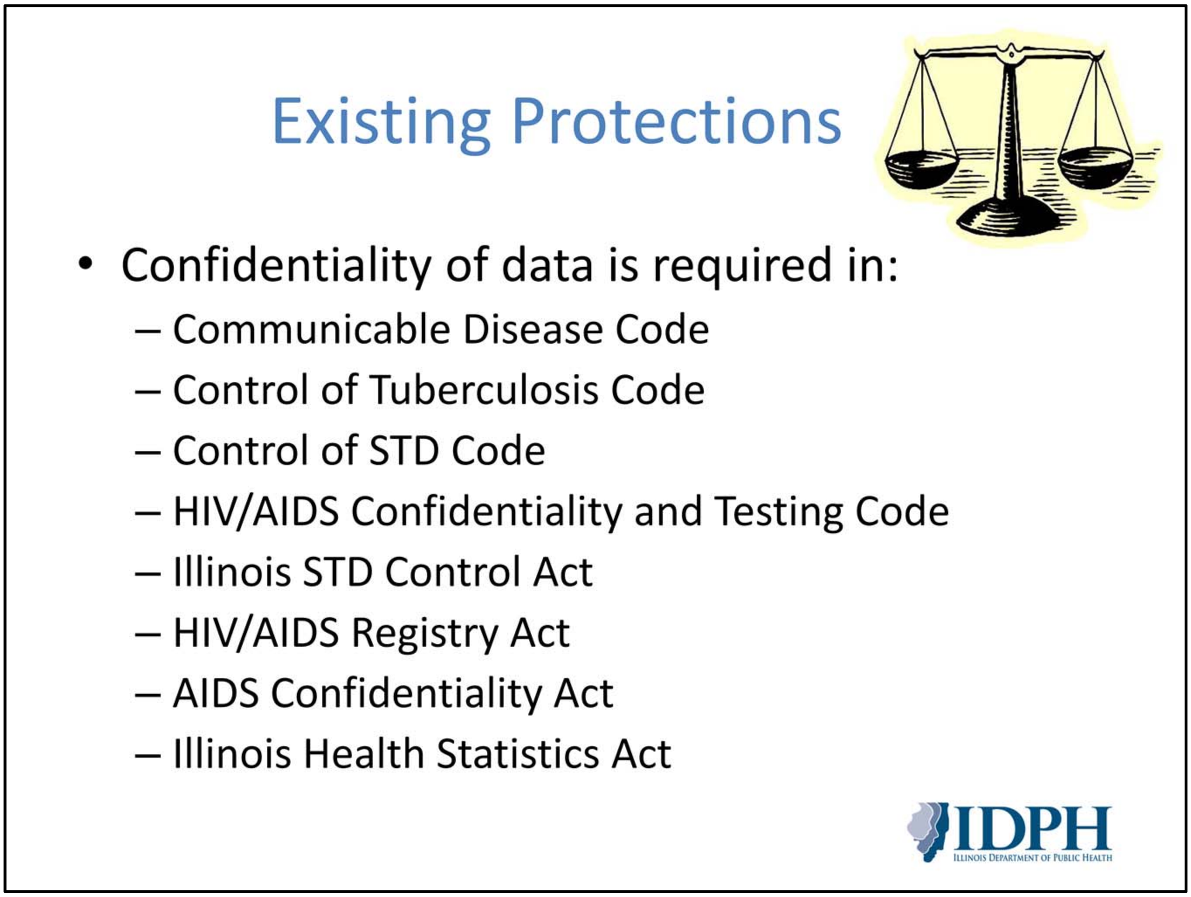
Applicable Parties

- Security and Confidentiality Guidelines define the standard of conduct that the public should expect of individuals who are responsible for protecting private and sensitive information.
  - ALL staff who handle confidential information are required to complete this training once every year.
    - This includes:
      - IDPH employees
      - Local health department staff
      - Public health designees (including community based organizations)
      - Temporary employees and student interns
      - Contractors/subcontractors
      - IT staff

IDPH
Illinois Department of Public Health

The Data Security and Confidentiality Guidelines define the standard of conduct that the public should expect of individuals who are responsible for protecting private and sensitive **Protected Health Information**.

It is required of ALL STAFF who handle confidential information to complete this training once every year. This includes all Illinois Department of Public Health employees, local health department staff, public health designees (including community based organizations), temporary employees and student interns, contractors and subcontractors, and IT staff who have access to confidential HIV or health information.

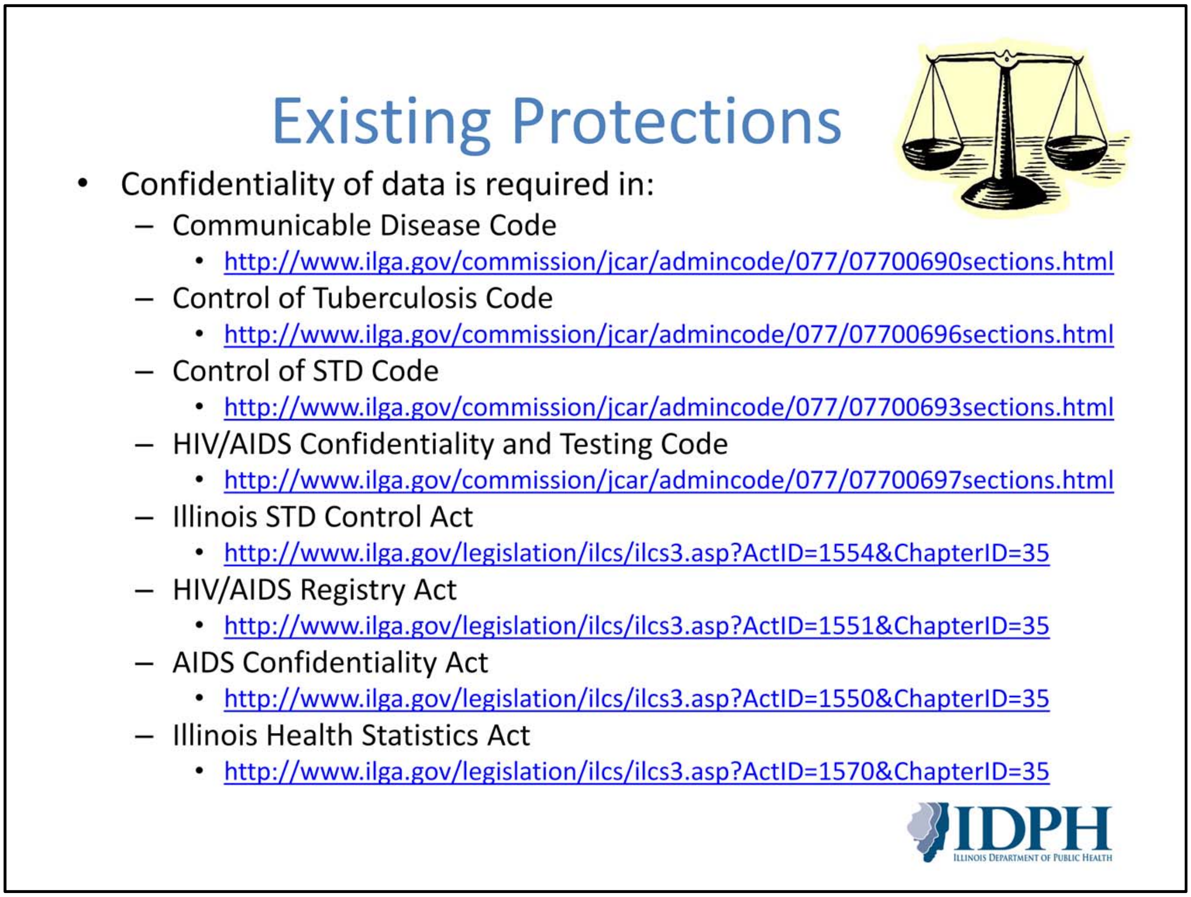


Existing Protections

- Confidentiality of data is required in:
  - Communicable Disease Code
  - Control of Tuberculosis Code
  - Control of STD Code
  - HIV/AIDS Confidentiality and Testing Code
  - Illinois STD Control Act
  - HIV/AIDS Registry Act
  - AIDS Confidentiality Act
  - Illinois Health Statistics Act

State statutes and administrative rules shown here address the legal protection of health-related data. Each statute and rule outlines in specific detail confidentiality requirements for programs that collect data and identifies responsible parties and/or entities for reporting such data sets to local and state public health officials. These protections also include measures to safeguard all information and records held by the state and local health departments as well as their authorized representatives. The HIV and STD rule sets also specify strict confidential requirements, including exemptions from inspection under the Freedom of Information Act.

As we'll cover in the following sections of this training, programs should always first ask, "Do I have the authority to collect information and/or release it?" These rules specify those data collection and release rules.

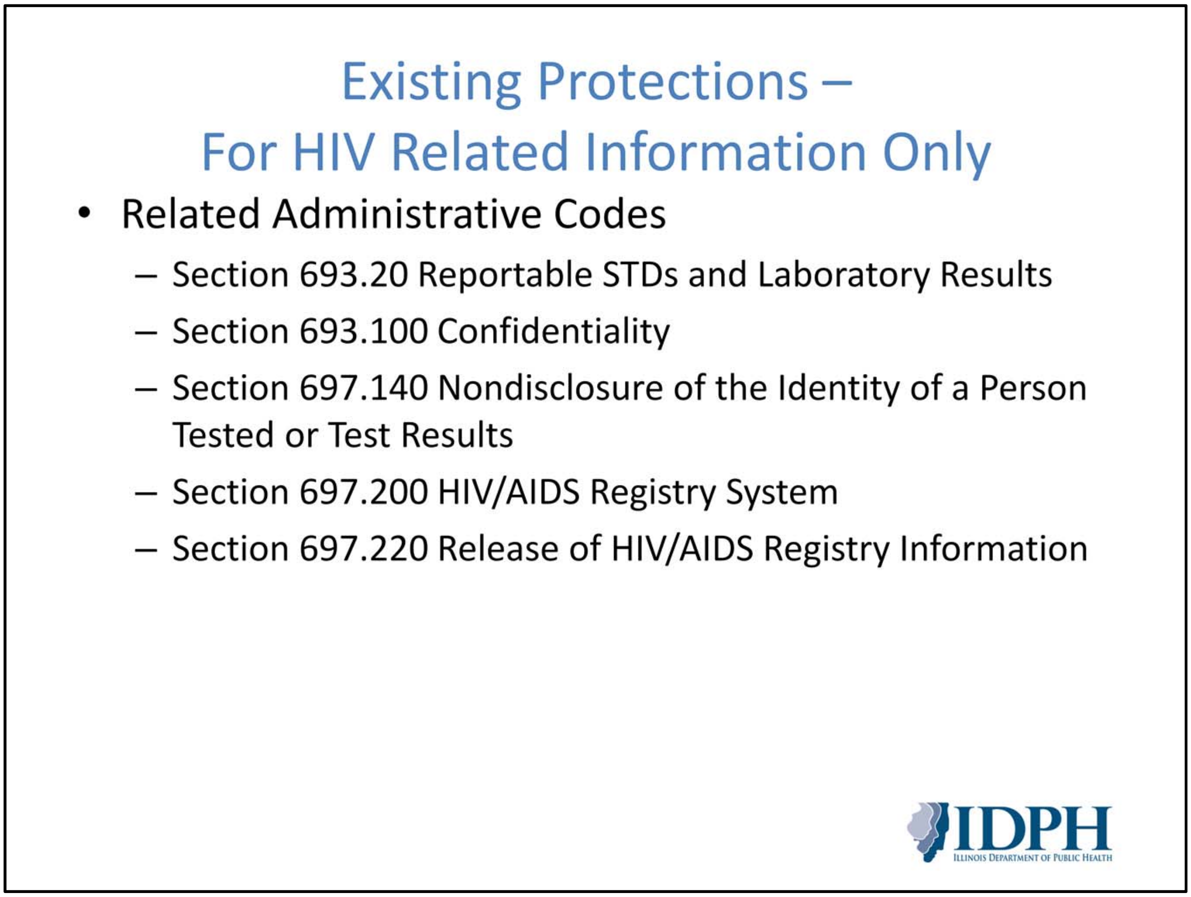


Existing Protections

- Confidentiality of data is required in:
  - Communicable Disease Code
    - http://www.ilga.gov/commission/jcar/admincode/077/07700690sections.html
  - Control of Tuberculosis Code
    - http://www.ilga.gov/commission/jcar/admincode/077/07700696sections.html
  - Control of STD Code
    - http://www.ilga.gov/commission/jcar/admincode/077/07700693sections.html
  - HIV/AIDS Confidentiality and Testing Code
    - http://www.ilga.gov/commission/jcar/admincode/077/07700697sections.html
  - Illinois STD Control Act
    - http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1554&ChapterID=35
  - HIV/AIDS Registry Act
    - http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1551&ChapterID=35
  - AIDS Confidentiality Act
    - http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1550&ChapterID=35
  - Illinois Health Statistics Act
    - http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1570&ChapterID=35

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

For more information, please visit the corresponding link.

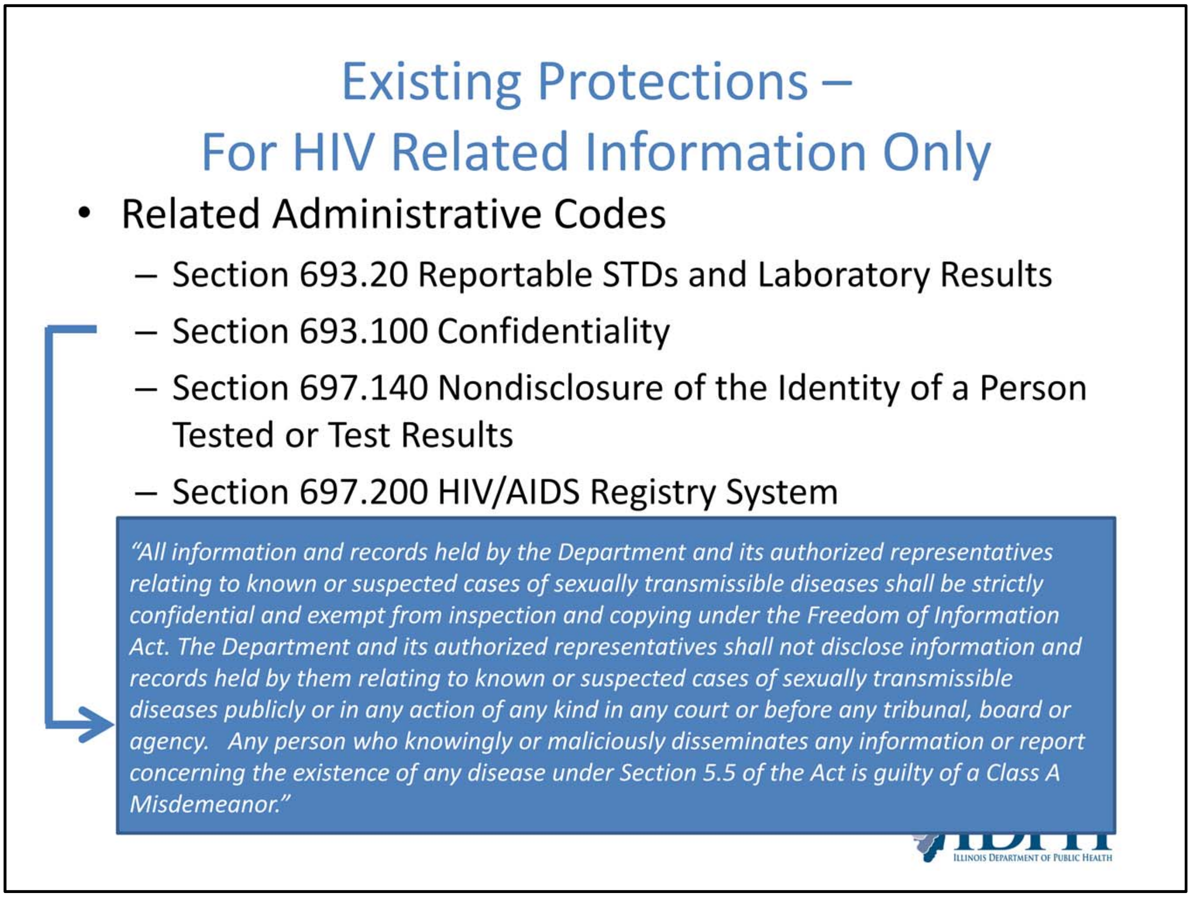


Existing Protections – For HIV Related Information Only

- Related Administrative Codes
  - Section 693.20 Reportable STDs and Laboratory Results
  - Section 693.100 Confidentiality
  - Section 697.140 Nondisclosure of the Identity of a Person Tested or Test Results
  - Section 697.200 HIV/AIDS Registry System
  - Section 697.220 Release of HIV/AIDS Registry Information

Let’s review the specific sections of the Administrative Rules that relate to HIV reporting and confidentiality.

Section 693.20 Describes all of the STDs and STD test results that the Illinois Department of Public Health requires all doctors, hospitals and other medical professionals to report to Local Health Departments and IDPH.



Existing Protections – For HIV Related Information Only

- Related Administrative Codes
  - Section 693.20 Reportable STDs and Laboratory Results
  - Section 693.100 Confidentiality
  - Section 697.140 Nondisclosure of the Identity of a Person Tested or Test Results
  - Section 697.200 HIV/AIDS Registry System

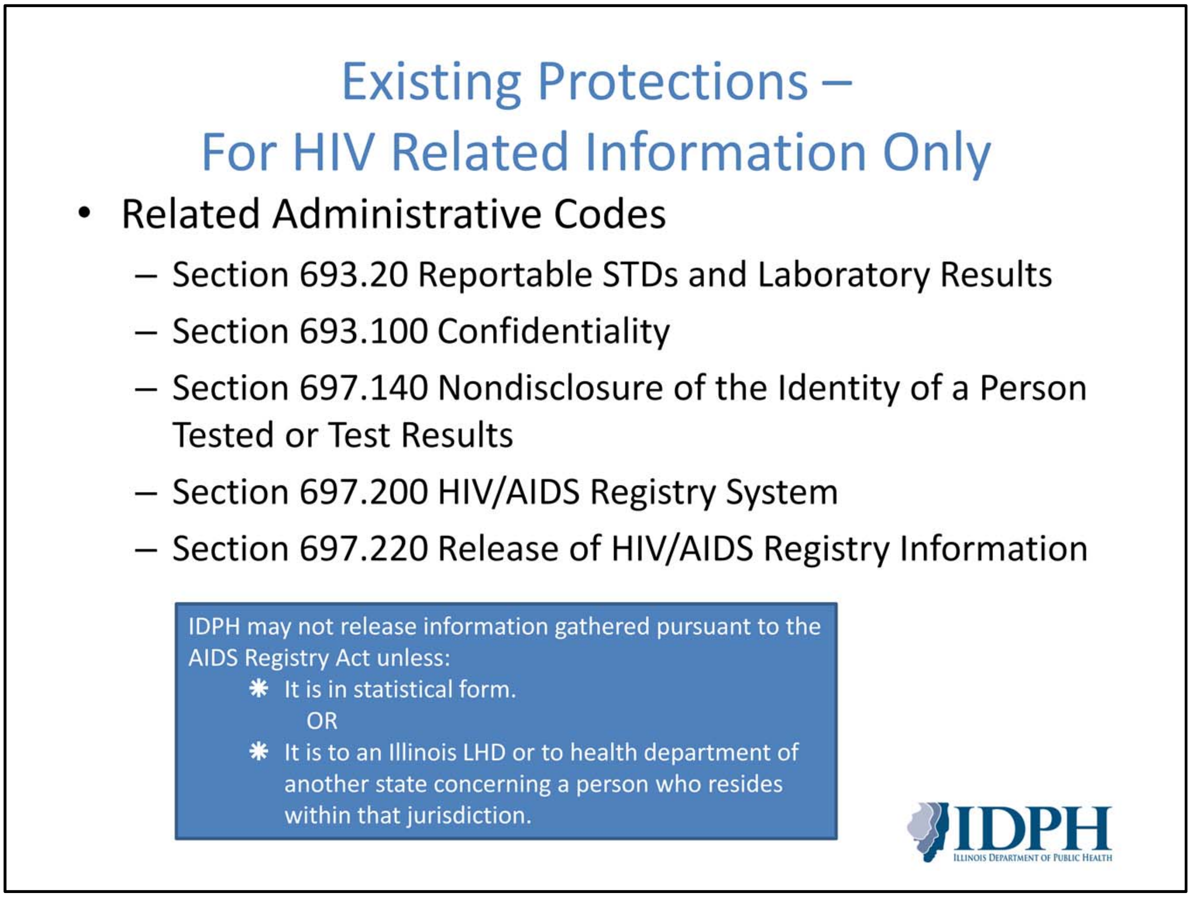
"All information and records held by the Department and its authorized representatives relating to known or suspected cases of sexually transmissible diseases shall be strictly confidential and exempt from inspection and copying under the Freedom of Information Act. The Department and its authorized representatives shall not disclose information and records held by them relating to known or suspected cases of sexually transmissible diseases publicly or in any action of any kind in any court or before any tribunal, board or agency. Any person who knowingly or maliciously disseminates any information or report concerning the existence of any disease under Section 5.5 of the Act is guilty of a Class A Misdemeanor."

IDPH ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Section 693.100 Describes the information IDPH identifies as confidential information. It also describes how information can and can not be released. It also explains the consequences for knowingly or maliciously releasing the information. Specifically, Section 693.100 reads:

> *All information and records held by the Department and its authorized representatives relating to known or suspected cases of sexually transmissible diseases shall be strictly confidential and exempt from inspection and copying under the Freedom of Information Act. The Department and its authorized representatives shall not disclose information and records held by them relating to known or suspected cases of sexually transmissible diseases publicly or in any action of any kind in any court or before any tribunal, board or agency.*
> *Any person who knowingly or maliciously disseminates any information or report concerning the existence of any disease under* Section 5.5 of the Act *is guilty of a Class A Misdemeanor.*

Section 697.140 Describes who is and who is not authorized to receive information regarding the test or results of a test for HIV. It also identifies the punishment for releasing such information without permission.



Existing Protections – For HIV Related Information Only

- Related Administrative Codes
  - Section 693.20 Reportable STDs and Laboratory Results
  - Section 693.100 Confidentiality
  - Section 697.140 Nondisclosure of the Identity of a Person Tested or Test Results
  - Section 697.200 HIV/AIDS Registry System
  - Section 697.220 Release of HIV/AIDS Registry Information

IDPH may not release information gathered pursuant to the AIDS Registry Act unless:

- ❋ It is in statistical form.
  OR
- ❋ It is to an Illinois LHD or to health department of another state concerning a person who resides within that jurisdiction.

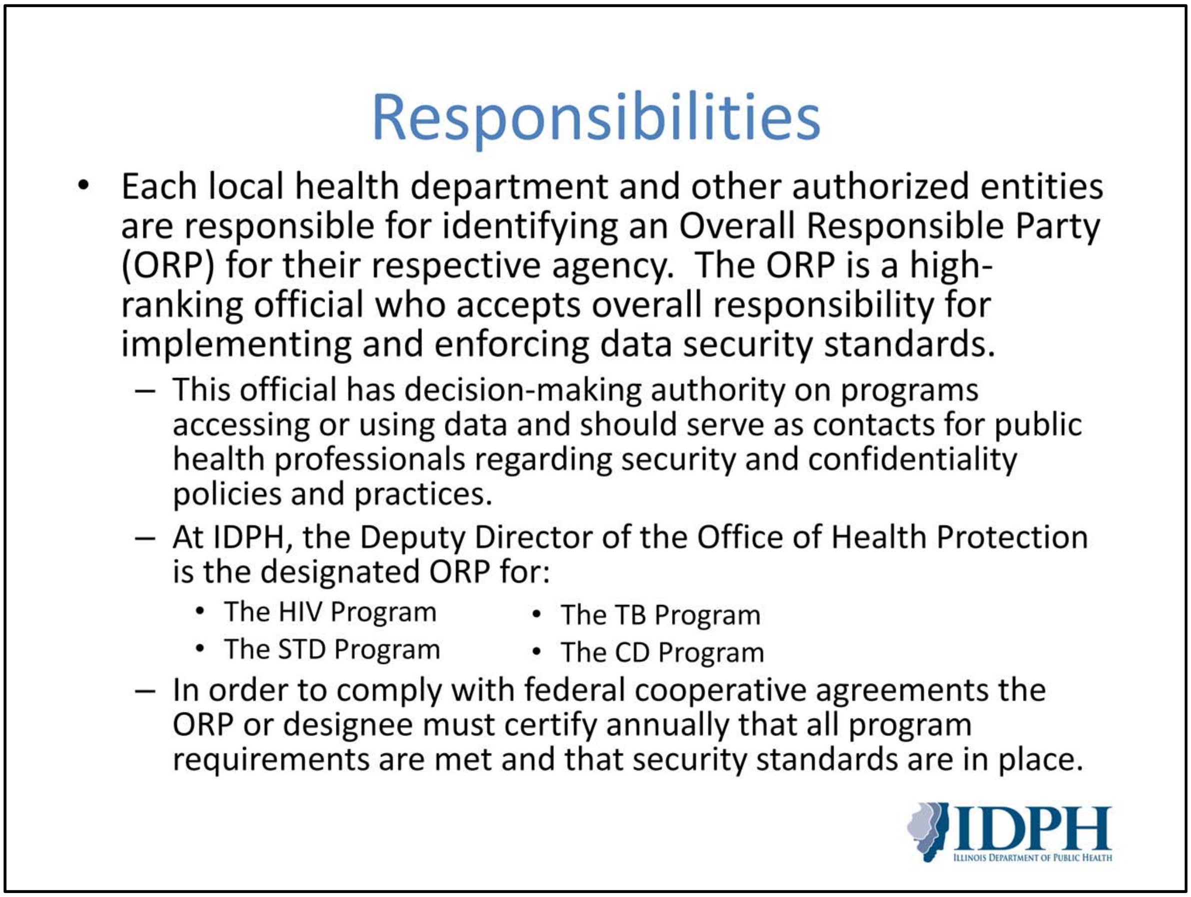
IDPH
Illinois Department of Public Health

Section 697.200 Gives the HIV/AIDS section the authority to compile and complete statistical data for HIV+ people in Illinois.

Section 697.220 Describes the rules related to HIV information contained in the HIV/AIDS Registry. All data obtained directly from medical records of individual patients shall be for the confidential use of IDPH and its authorized entities to view such records in order to carry out the purpose of the Registry Act.
Specifically:
IDPH does not release information gathered pursuant to the AIDS Registry Act unless:

It is in statistical form OR

It is to an Illinois LHD or to health department of another state, and is of information concerning a person who is residing within that jurisdiction.



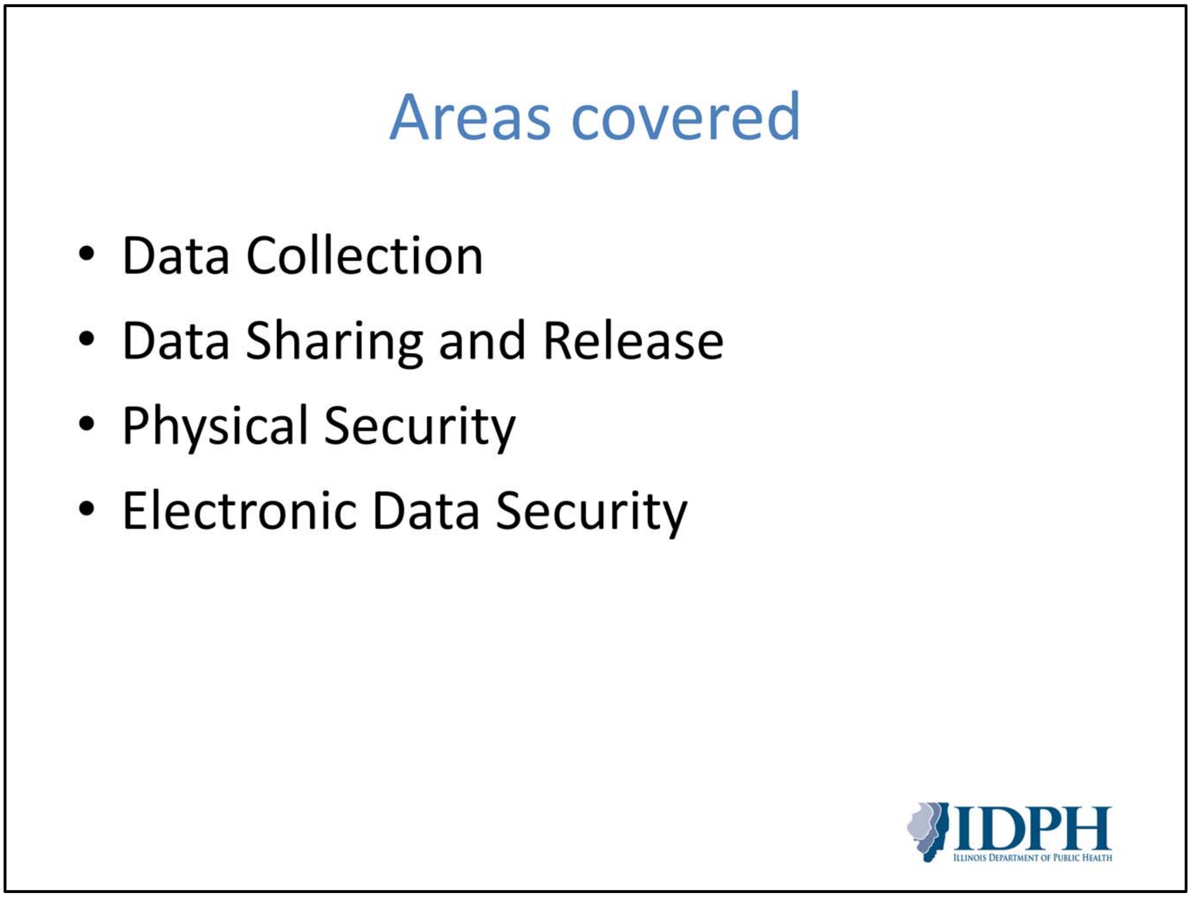
Responsibilities

- Each local health department and other authorized entities are responsible for identifying an Overall Responsible Party (ORP) for their respective agency. The ORP is a high-ranking official who accepts overall responsibility for implementing and enforcing data security standards.
  - This official has decision-making authority on programs accessing or using data and should serve as contacts for public health professionals regarding security and confidentiality policies and practices.
  - At IDPH, the Deputy Director of the Office of Health Protection is the designated ORP for:
    - The HIV Program
    - The STD Program
    - The TB Program
    - The CD Program
  - In order to comply with federal cooperative agreements the ORP or designee must certify annually that all program requirements are met and that security standards are in place.

IDPH
Illinois Department of Public Health

Each local health department and other authorized entities are responsible for identifying an Overall Responsible Party (otherwise know as ORP) for their respective agency. The ORP is a high-ranking official who accepts overall responsibility for implementing and enforcing data security standards. This official should have the authority to make decisions about program operations that might affect programs accessing or using the data, and should serve as contacts for public health professionals regarding security and confidentiality policies and practices.

The Deputy Director of the Illinois Department of Public Health Office of Health Protection is the designated ORP for the HIV, STD, TB and CD Program. The ORP is responsible for the security and confidentiality of data and has the authority to make decisions about program operations. In compliance with CDC cooperative agreement requirements, the ORP will certify annually that all program requirements are met, that security standards are in place, and has approved the policies outlined in this training.



Areas covered

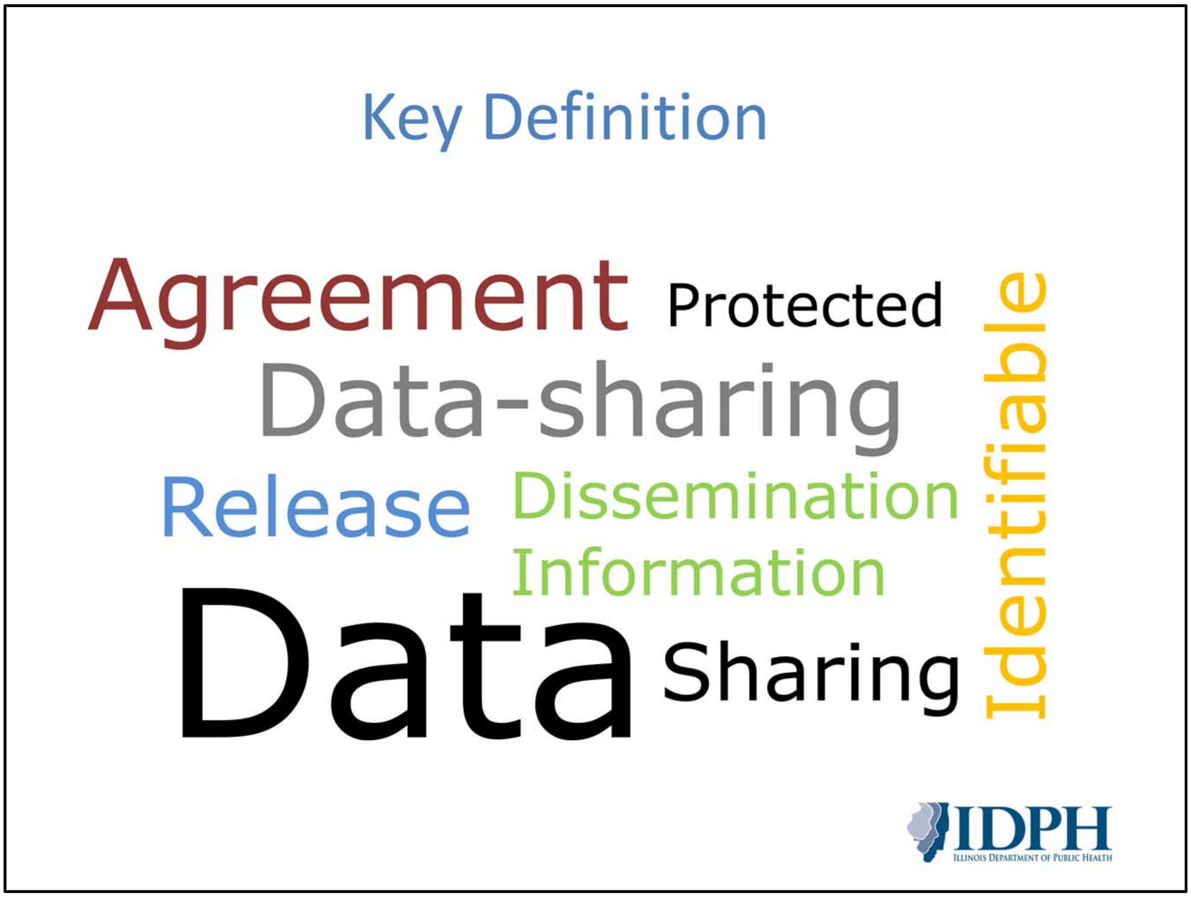
- Data Collection
- Data Sharing and Release
- Physical Security
- Electronic Data Security

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Areas that we will cover in the next section include:
Data Collection
Data Sharing and Release
Physical Security and
Electronic Data Security

DEFINITIONS

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH



Key Definition

Agreement Protected

Data-sharing

Release Dissemination

Information

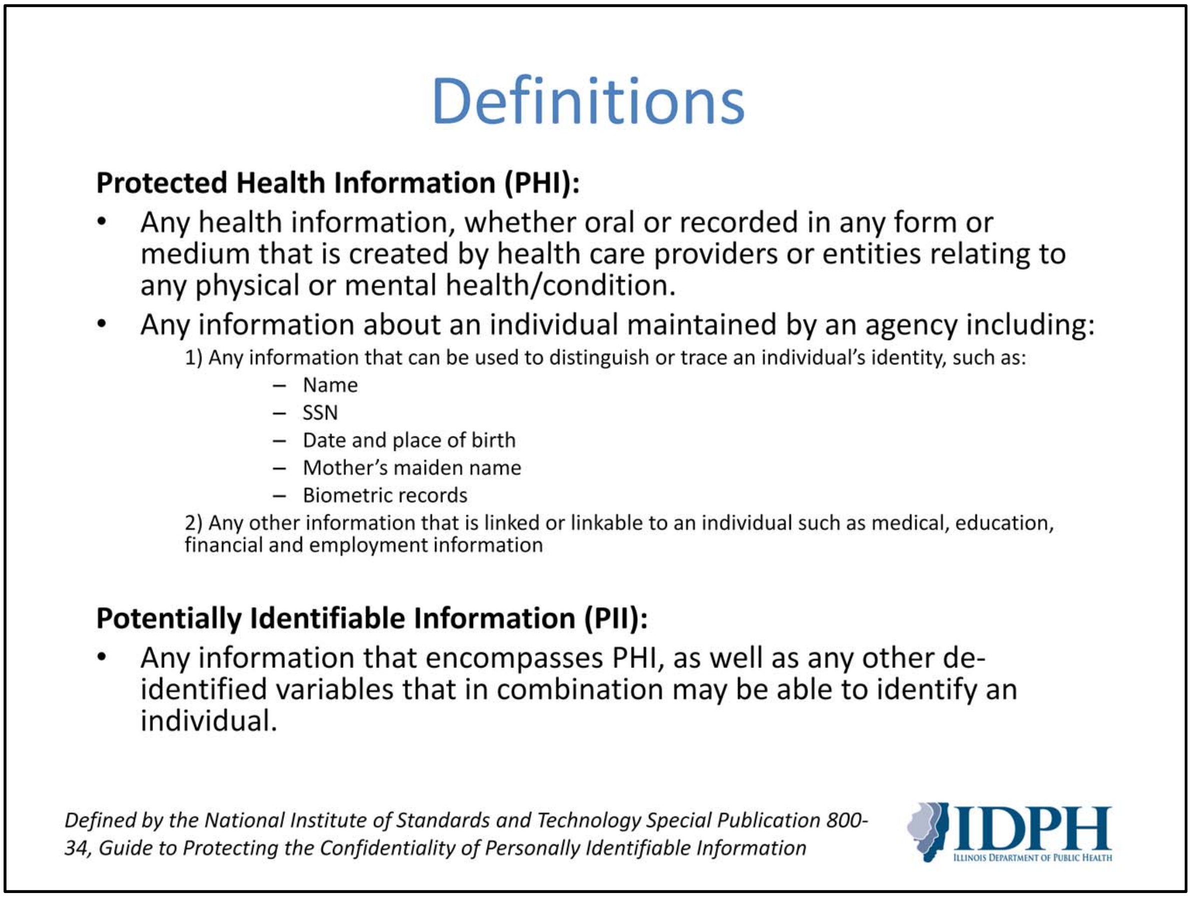
Data Sharing

Identifiable

IDPH

Illinois Department of Public Health

In the next set of slides, we will be reviewing definitions of key words used in the guidelines.



Definitions

Protected Health Information (PHI):

- Any health information, whether oral or recorded in any form or medium that is created by health care providers or entities relating to any physical or mental health/condition.
- Any information about an individual maintained by an agency including:

  1) Any information that can be used to distinguish or trace an individual's identity, such as:
     - Name
     - SSN
     - Date and place of birth
     - Mother's maiden name
     - Biometric records

  2) Any other information that is linked or linkable to an individual such as medical, education, financial and employment information

Potentially Identifiable Information (PII):

- Any information that encompasses PHI, as well as any other de-identified variables that in combination may be able to identify an individual.

Defined by the National Institute of Standards and Technology Special Publication 800-34, Guide to Protecting the Confidentiality of Personally Identifiable Information

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Protected Health information, or PHI, includes any health information, whether oral or recorded in any form that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; *and*

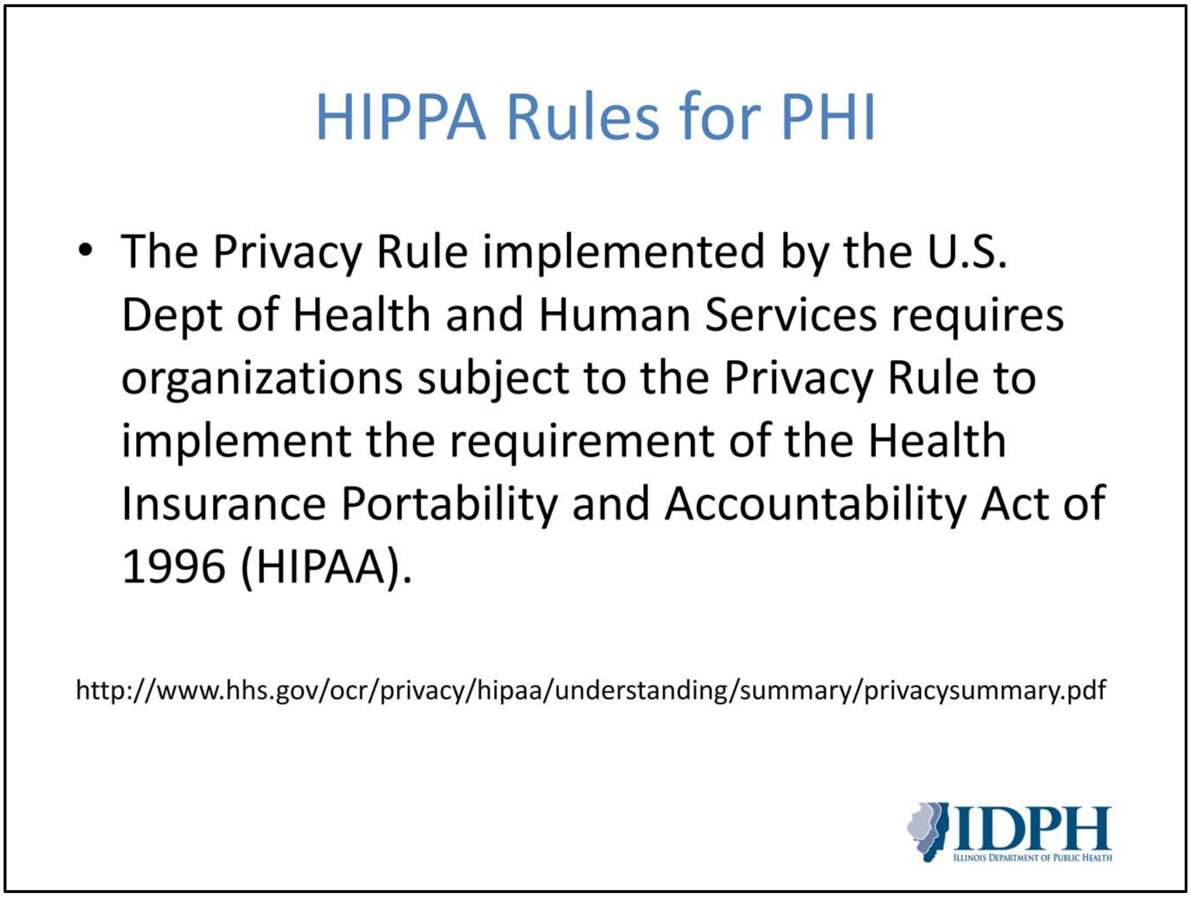
- Relates to the past, present, or

future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Examples include a person’s medical record, infection/disease case report form.

Potentially Identifiable Information, or PII, is any information that encompasses PHI, as well as any other de-identified variables that in combination may be able to identify an individual.

Examples include release information on a West Nile Virus death in a small county where the sex and age of the person are released. In this scenario, this information is potentially identifiable because the identity of this person could be determined by reading obituaries in the local paper or online.



HIPPA Rules for PHI

- The Privacy Rule implemented by the U.S. Dept of Health and Human Services requires organizations subject to the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

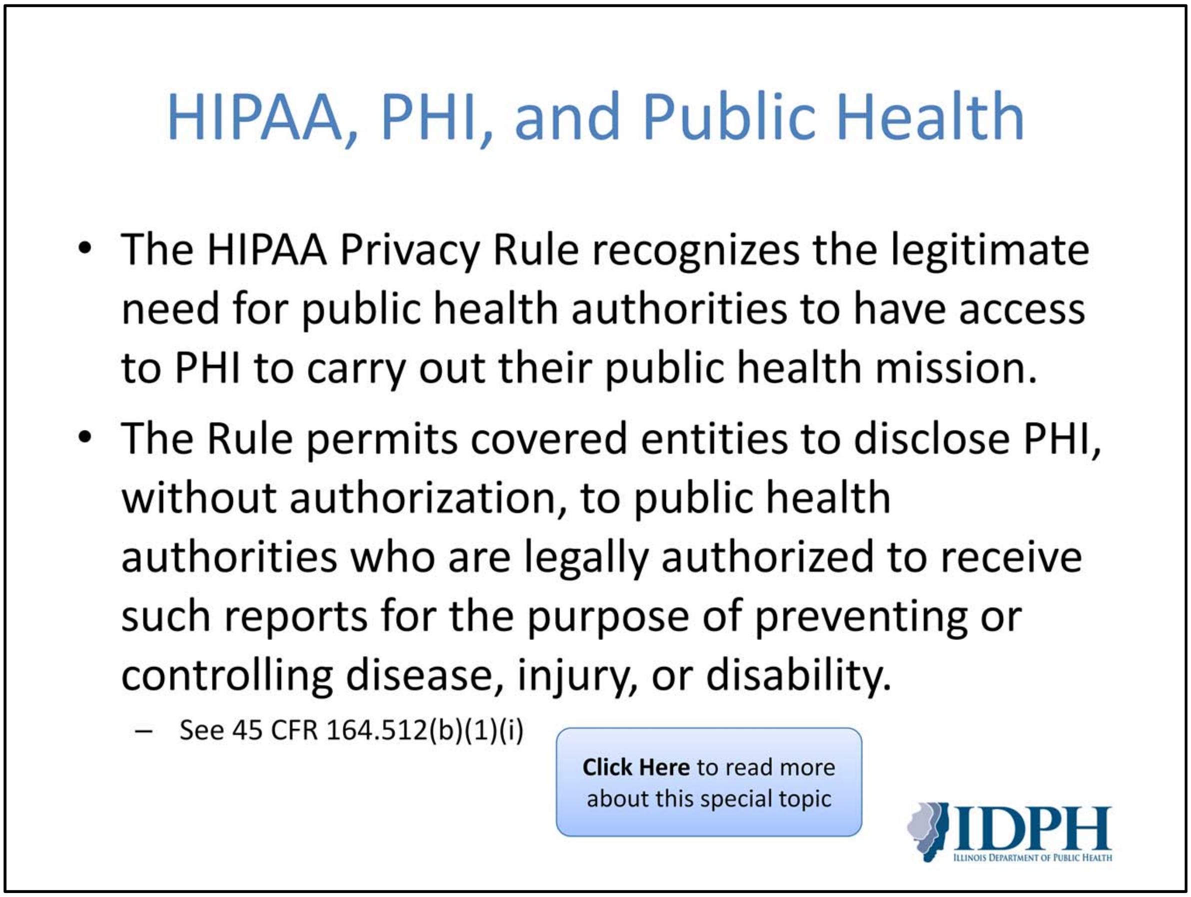
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

We will next discuss how HIPPA rules apply to data release, the use of PHI, and how it applies in Public Health.

The Privacy Rule implemented by the U.S. Dept of Health and Human Services requires health care providers, health care clearinghouses and health plans to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities.

The goal of the Privacy Rule is to assure the individual's health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.



HIPAA, PHI, and Public Health

- The HIPAA Privacy Rule recognizes the legitimate need for public health authorities to have access to PHI to carry out their public health mission.
- The Rule permits covered entities to disclose PHI, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.
  - See 45 CFR 164.512(b)(1)(i)

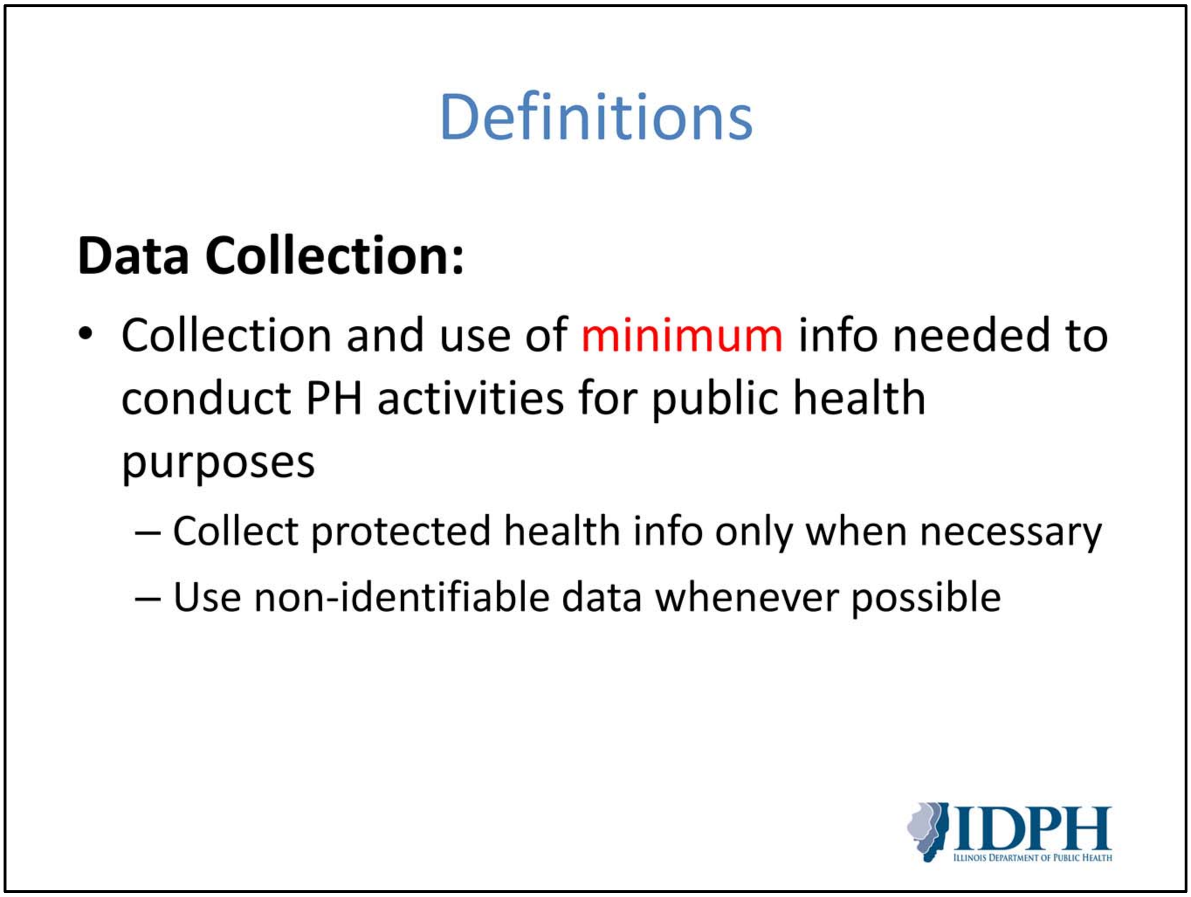
Click Here to read more about this special topic

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities to have access to PHI to carry out the public health mission.

The Rule permits covered entities, such as health care providers, to disclose PHI, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This includes: the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions.

For more information on HIPAA and a copy of the HIPAA law can be found on the U.S. Department of Health and Human Services website.

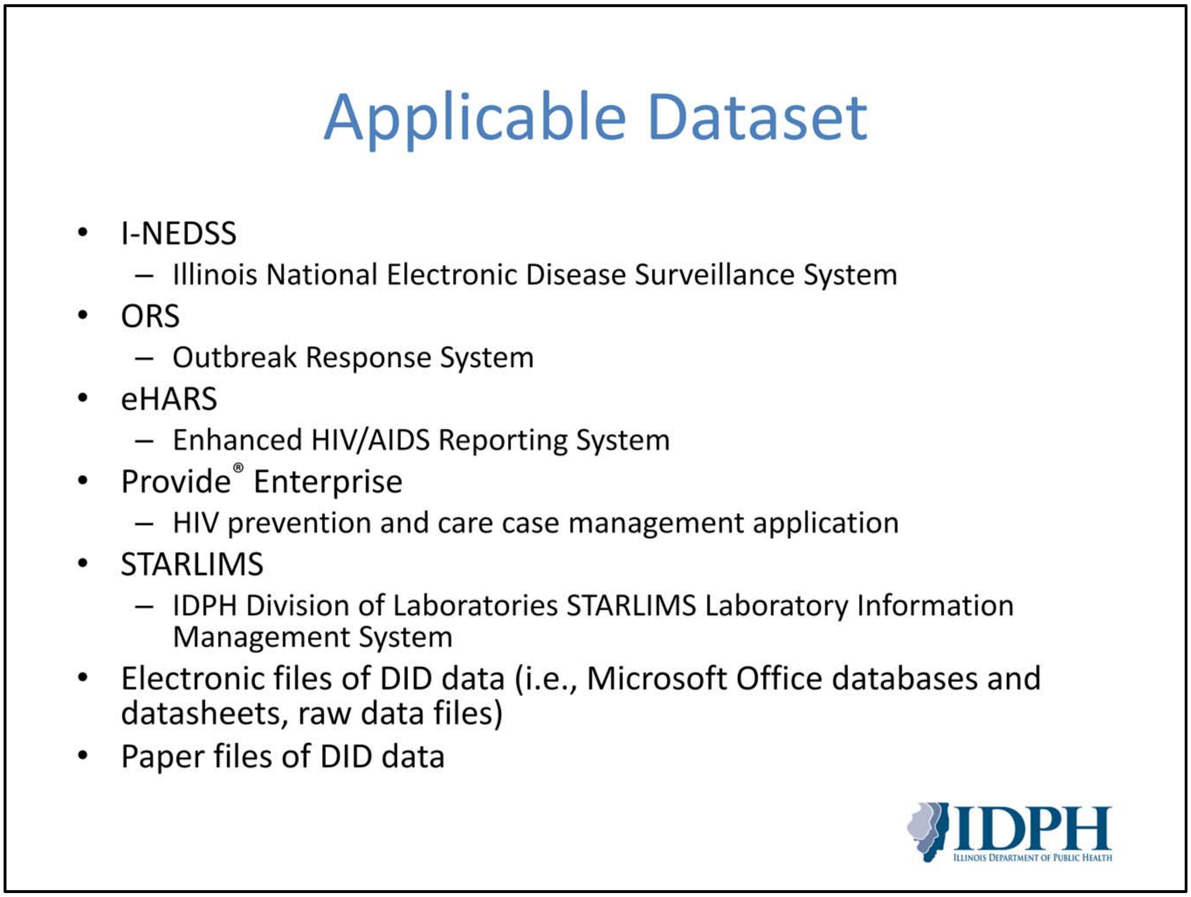


Definitions

Data Collection:

- Collection and use of minimum info needed to conduct PH activities for public health purposes
  - Collect protected health info only when necessary
  - Use non-identifiable data whenever possible

The term Data Collection, when referring to health information, is the process of gathering and measuring information on variables of interest that are needed to conduct public health activities for public health purposes. Collection of **protected health information** should only be done when necessary and/or required by law. Whenever possible, it is recommended to use non-identifiable data fields to carry out public health activities.

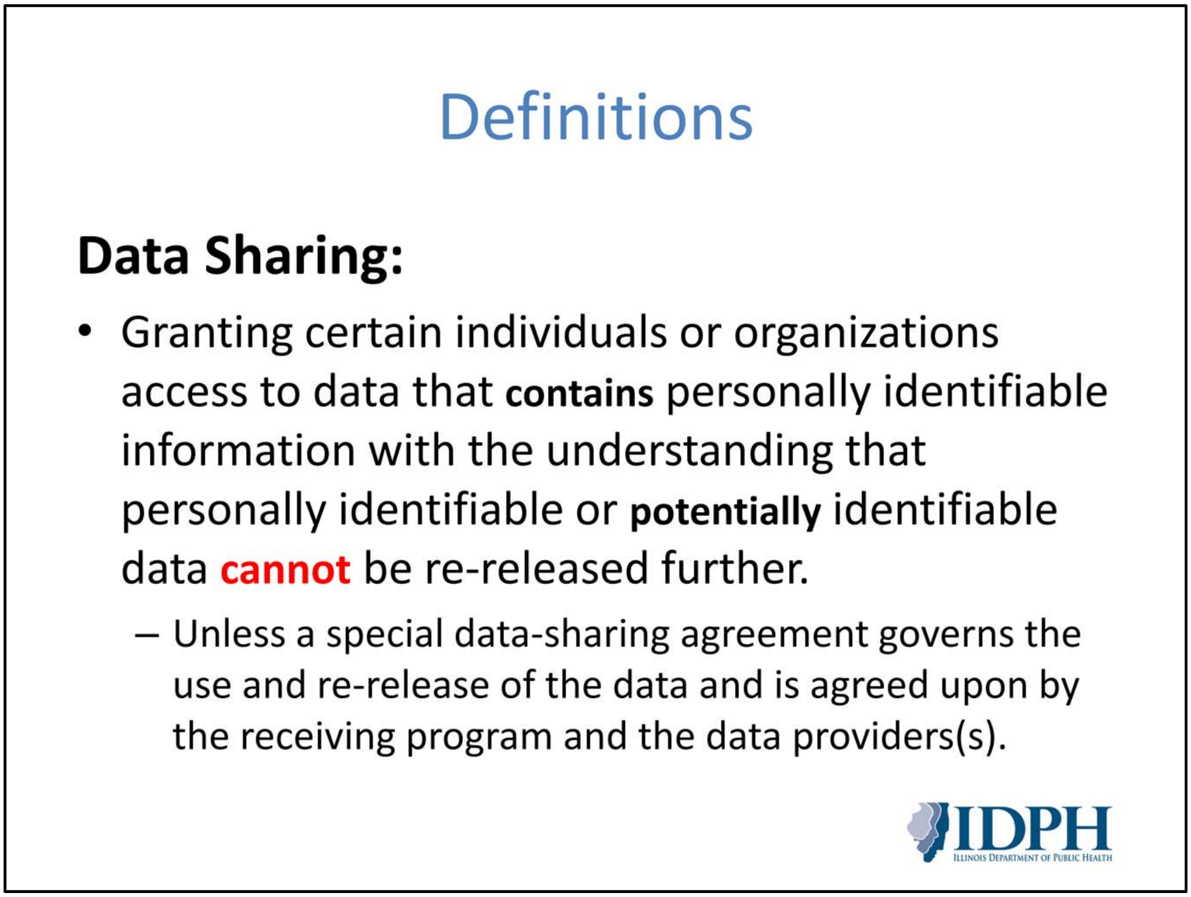


Applicable Dataset

- I-NEDSS
  - Illinois National Electronic Disease Surveillance System
- ORS
  - Outbreak Response System
- eHARS
  - Enhanced HIV/AIDS Reporting System
- Provide® Enterprise
  - HIV prevention and care case management application
- STARLIMS
  - IDPH Division of Laboratories STARLIMS Laboratory Information Management System
- Electronic files of DID data (i.e., Microsoft Office databases and datasheets, raw data files)
- Paper files of DID data

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Applications used by the IL Department of Public Health Office of Health Protection to manage various health records and data sets include:
INEDSS, ORS, eHARS, Provide Enterprise, STARLIMS and other electronic or paper files such as databases and spreadsheets.



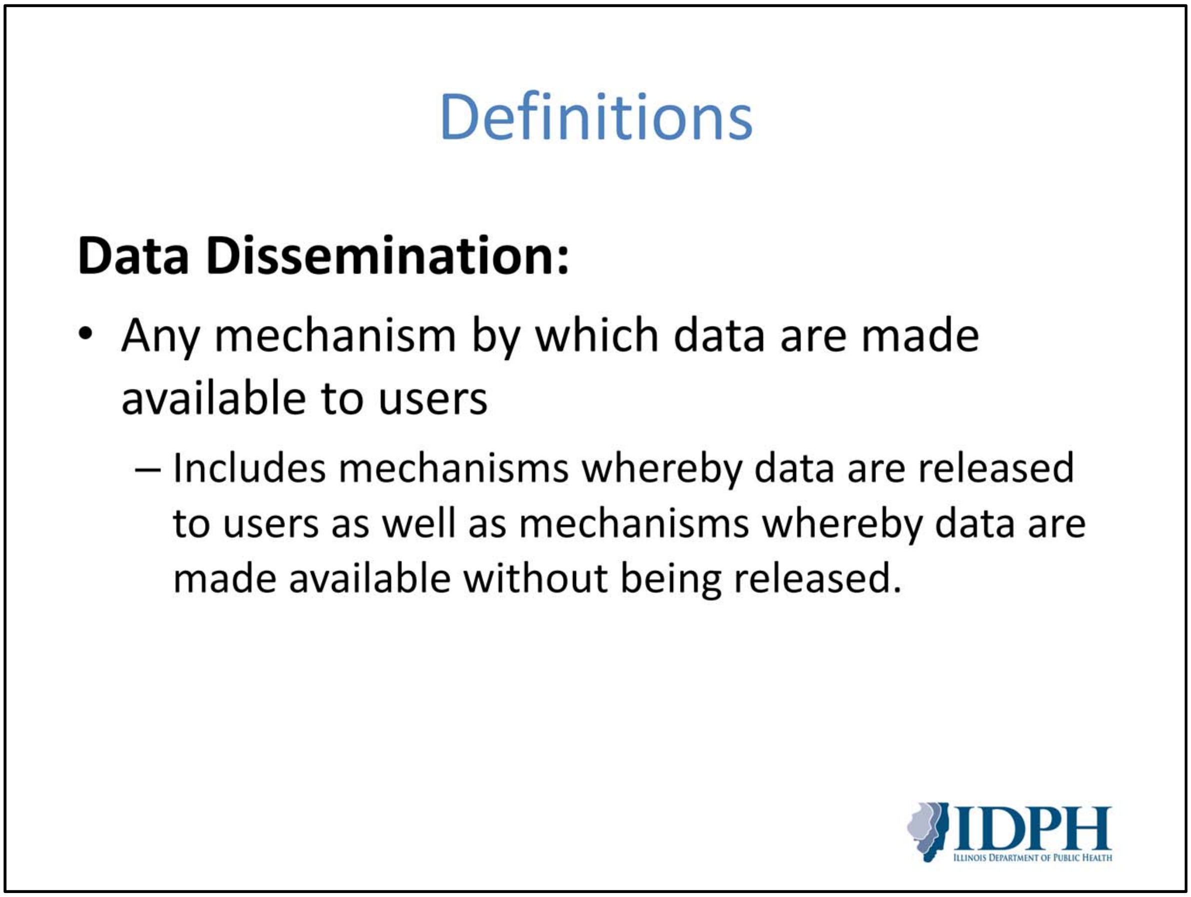
Definitions

Data Sharing:

- Granting certain individuals or organizations access to data that **contains** personally identifiable information with the understanding that personally identifiable or **potentially** identifiable data **cannot** be re-released further.
  - Unless a special data-sharing agreement governs the use and re-release of the data and is agreed upon by the receiving program and the data providers(s).

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Data sharing is defined as granting certain individuals or organizations access to data that contains **personally** identifiable information with the understanding that personally identifiable or **potentially** identifiable data **cannot** be re-released further. In some instances, this data can be re-released to additional covered entities for public health and surveillance purposes under the condition that a special data-sharing agreement or contract is in place that is agreed upon by the receiving program and all data provider(s).



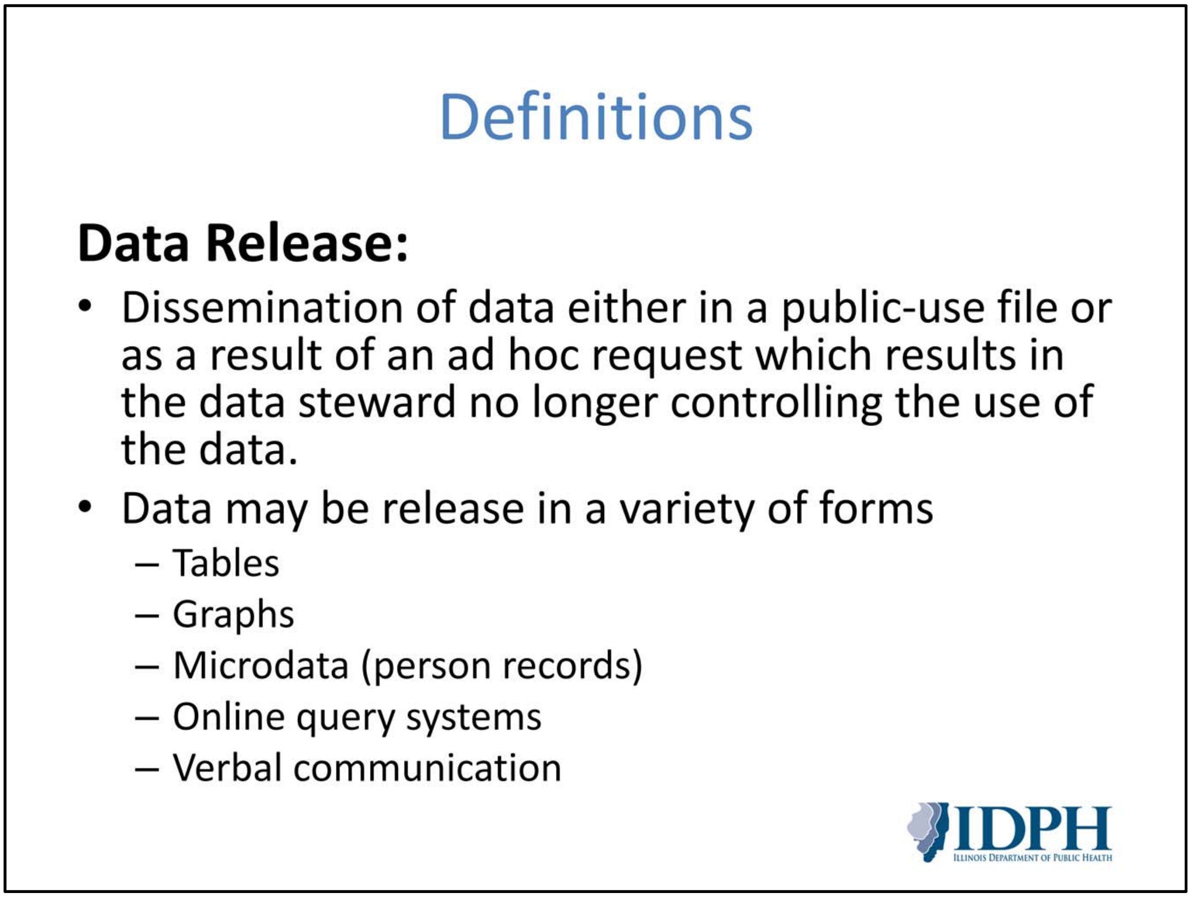
Definitions

Data Dissemination:

- Any mechanism by which data are made available to users
  - Includes mechanisms whereby data are released to users as well as mechanisms whereby data are made available without being released.

Data Dissemination is defined as any mechanism by which data are made available to users. For example, reporting electronic and paper reporting documents to local health departments **for protecting the health of citizens**. This can act as a vehicle for improving the health of the community and for guiding LHD actions in support of policy changes and to improve public health programs.

Dissemination covers areas regarding how the data is released to users such as LHDs and how they will be made available without being released. Data Released will be defined in the next slide.



Definitions

Data Release:

- Dissemination of data either in a public-use file or as a result of an ad hoc request which results in the data steward no longer controlling the use of the data.
- Data may be release in a variety of forms
  - Tables
  - Graphs
  - Microdata (person records)
  - Online query systems
  - Verbal communication

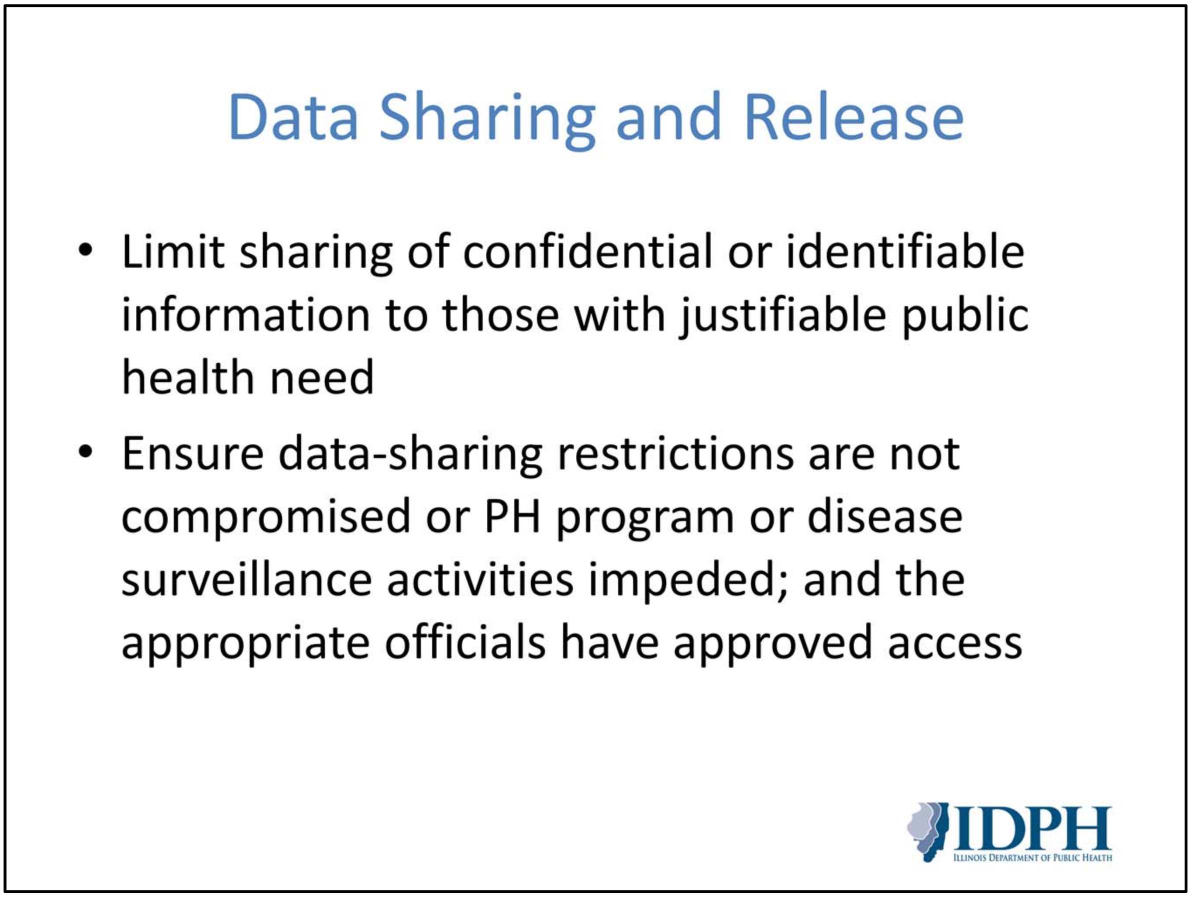
IDPH
Illinois Department of Public Health

Data release is defined as dissemination of data as a public-use file or as a result of an ad hoc request which results in the data steward no longer controlling the use of the data. Data can be released in a variety of forms such as in tables, graphs, microdata, online query systems, or verbal cmmunication.

DATA SHARING AND RELEASE

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

In the next few slides, we will discuss the sharing and release of confidential health data and information sets.

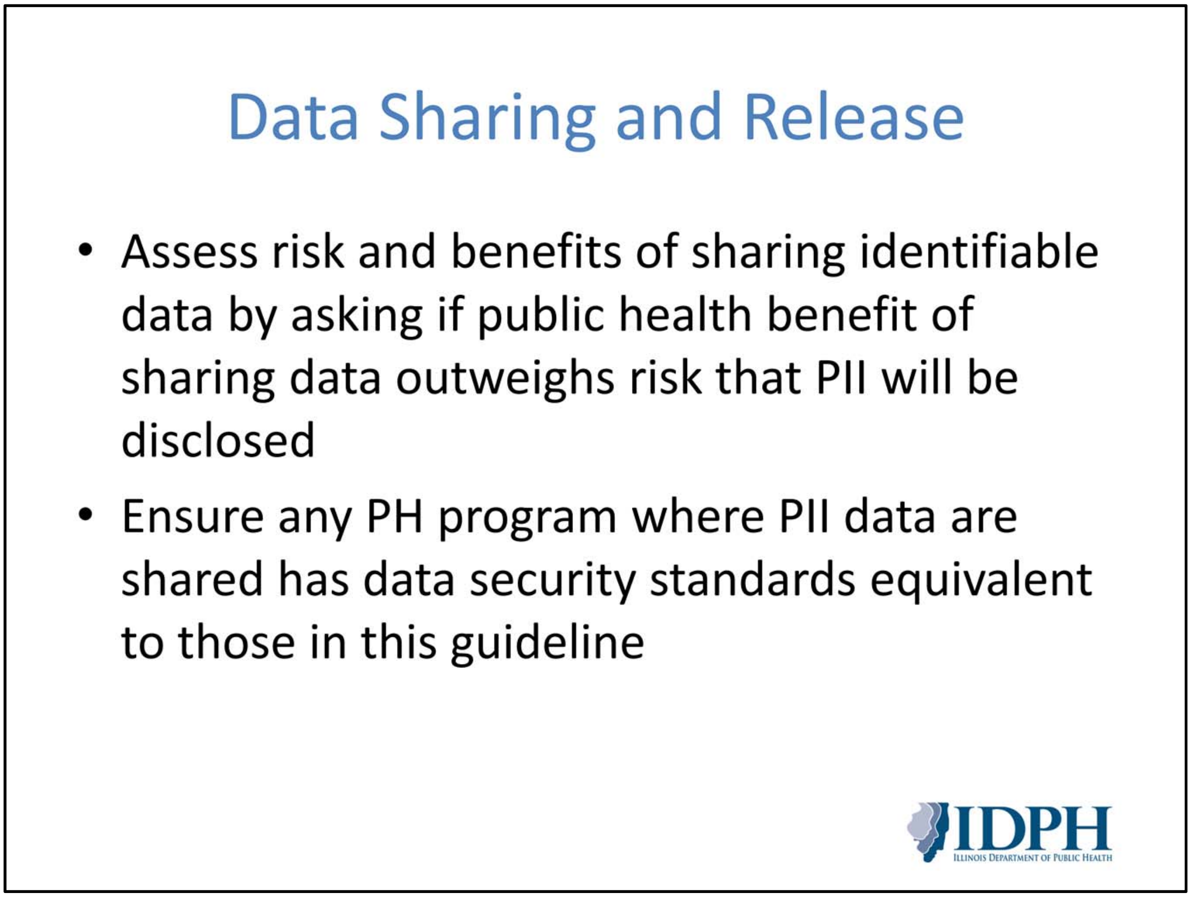


Data Sharing and Release

- Limit sharing of confidential or identifiable information to those with justifiable public health need
- Ensure data-sharing restrictions are not compromised or PH program or disease surveillance activities impeded; and the appropriate officials have approved access

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When sharing data, make an effort to limit the sharing of confidential or identifiable information to those entities/persons with a justifiable public health need. Make certain that data-sharing restrictions are not compromised or public health program or disease surveillance activities are not being impeded; and that the persons you are sharing this data with are the appropriate officials and have approved access



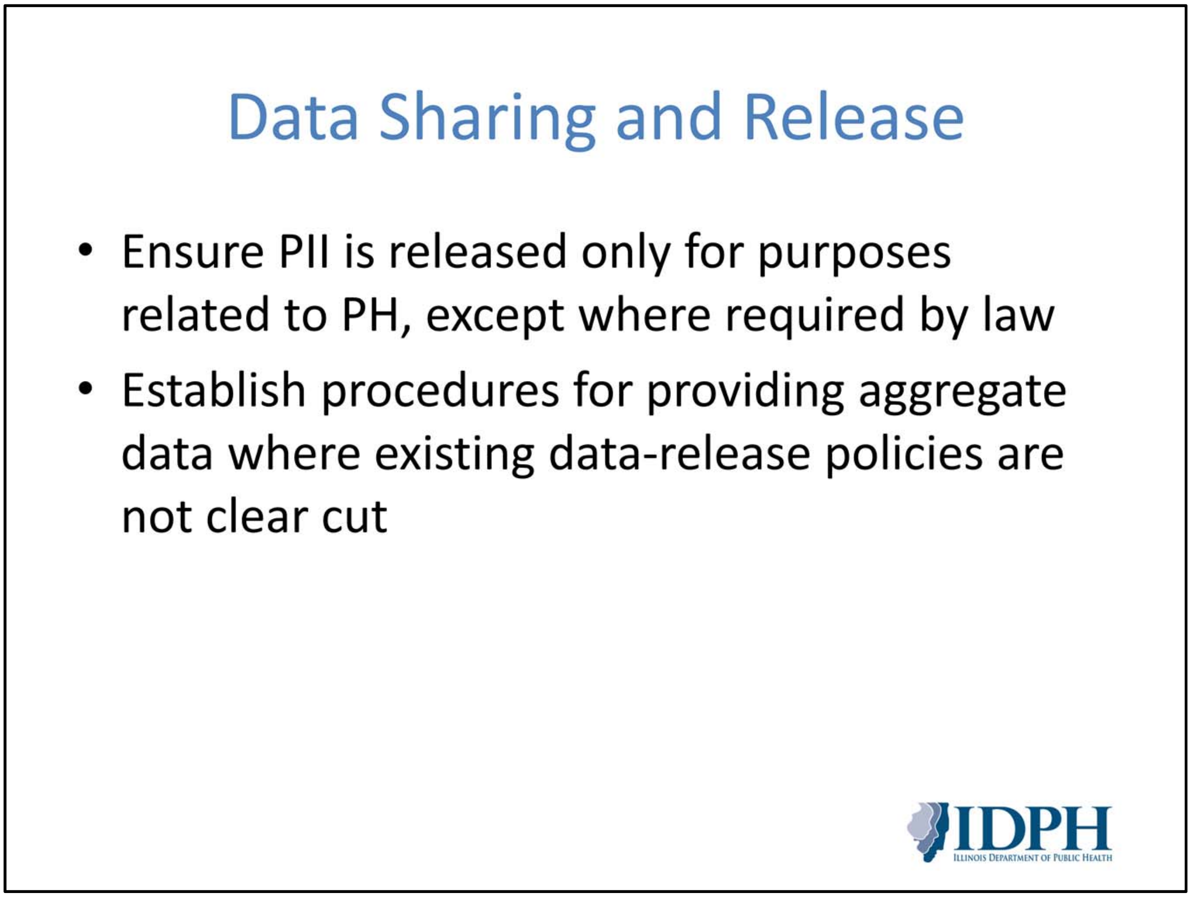
Data Sharing and Release

- Assess risk and benefits of sharing identifiable data by asking if public health benefit of sharing data outweighs risk that PII will be disclosed
- Ensure any PH program where PII data are shared has data security standards equivalent to those in this guideline

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When sharing confidential health data sets be sure to Assess risk and benefits of sharing identifiable data by asking the question, “Does the Public Health benefit of sharing data outweigh the risk that PII will be disclosed?”

Ensures that the public health program or entity you are sharing potentially identifiable information with has data security standards equivalent to those in this guideline



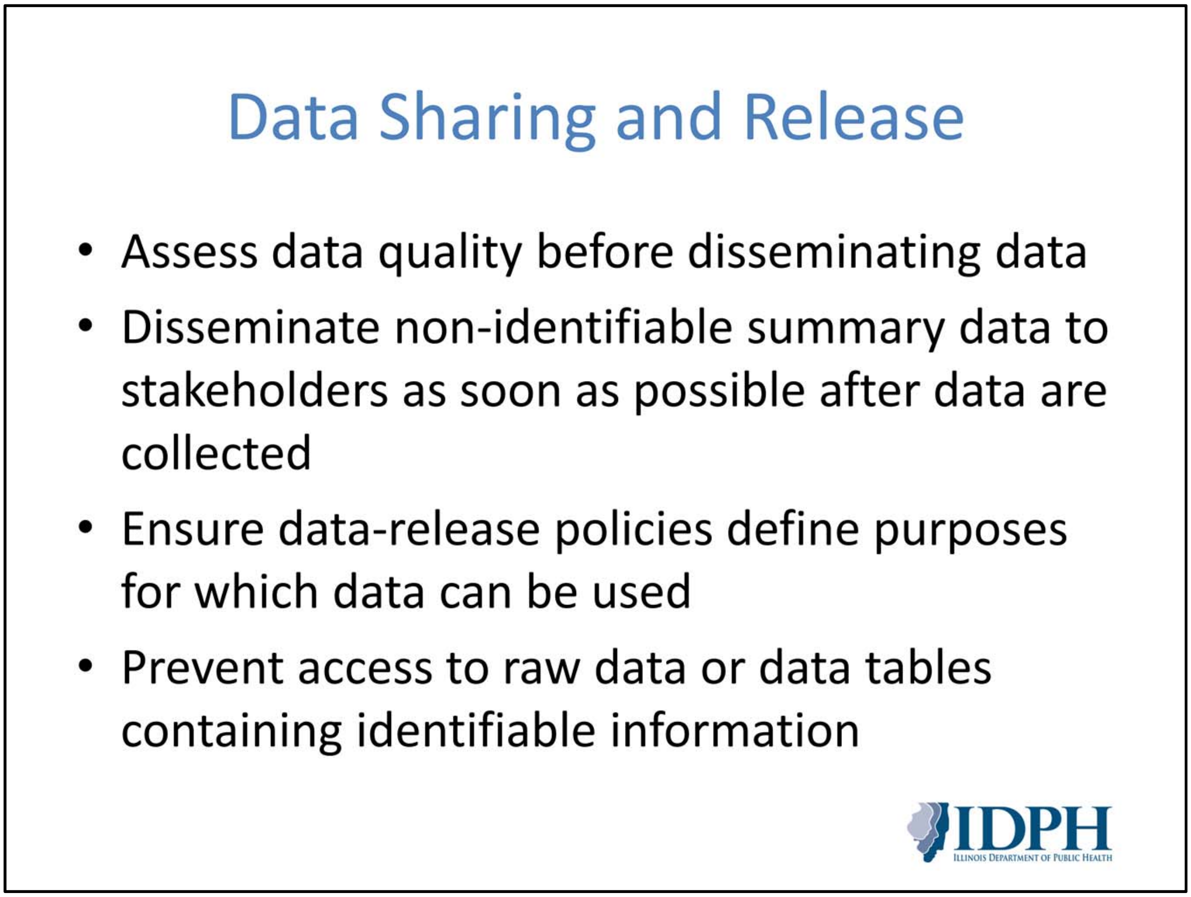
Data Sharing and Release

- Ensure PII is released only for purposes related to PH, except where required by law
- Establish procedures for providing aggregate data where existing data-release policies are not clear cut

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When releasing data with other public health programs or entities, it is recommended that one:
Make certain that the Potentially Identifiable Information is being released only for purposes related to Public Health activities, except where it is required by law.

And two, it is recommended that procedures are established for providing aggregate data where existing data-release policies are not clear cut.



Data Sharing and Release

- Assess data quality before disseminating data
- Disseminate non-identifiable summary data to stakeholders as soon as possible after data are collected
- Ensure data-release policies define purposes for which data can be used
- Prevent access to raw data or data tables containing identifiable information

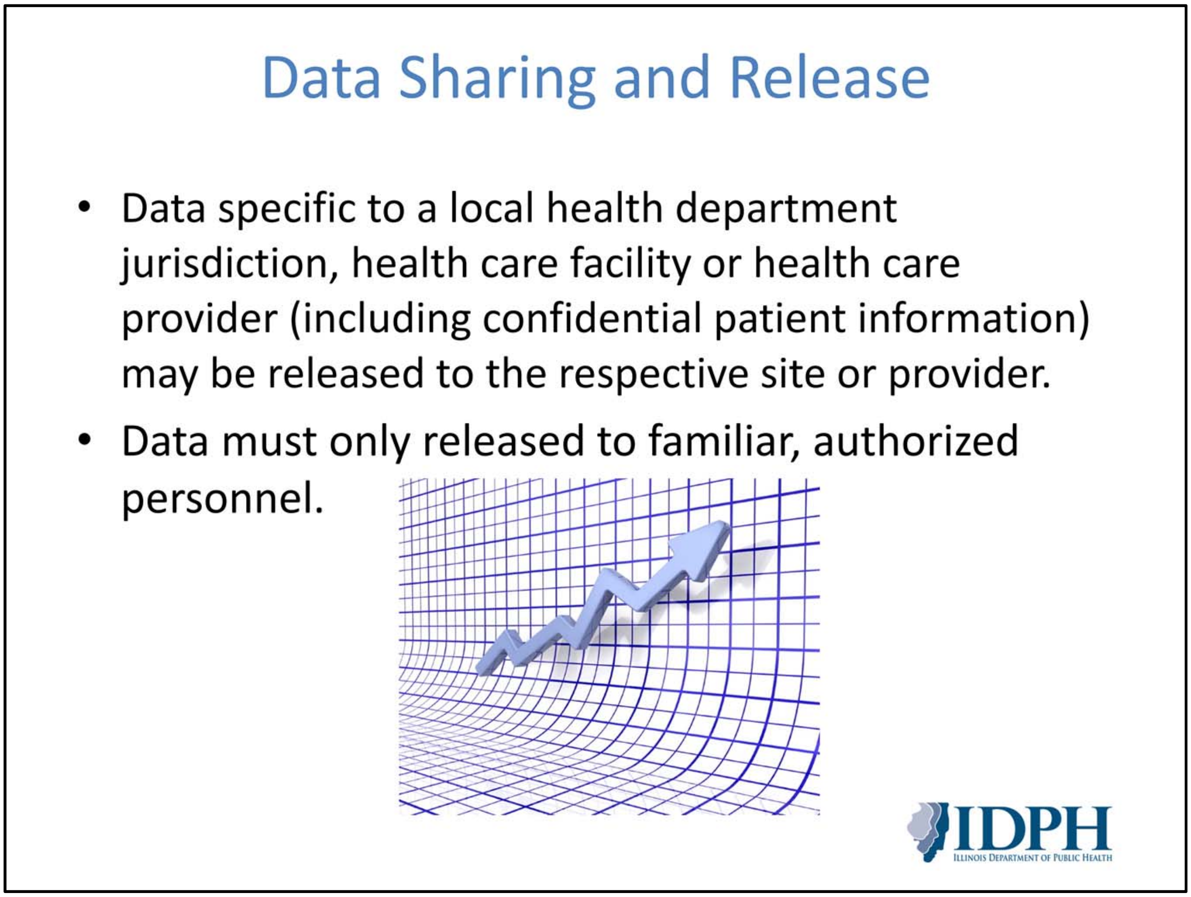
IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Prior to the releasing of data, one should:
Assess the data quality before disseminating to ensure you are providing accurate and appropriate information;

Disseminate non-identifiable summary data to stakeholders as soon as possible to continually ensure timely public health response;

Ensure data-release policies define purposes for which data can be used; and

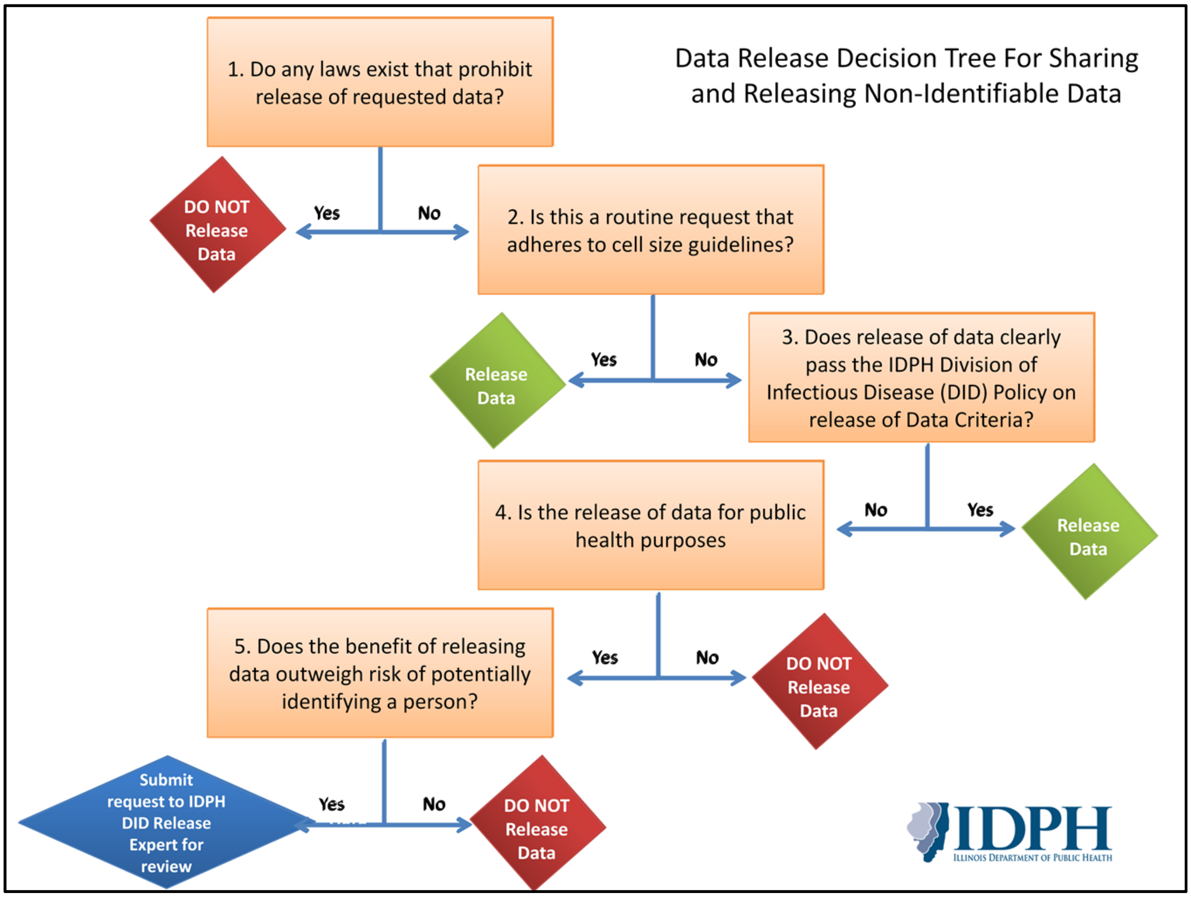
Prevent access to raw data or data tables containing identifiable information by adding additional security features such as password protections and encryptions. We will discuss this in greater detail later in the training.



Data Sharing and Release

- Data specific to a local health department jurisdiction, health care facility or health care provider (including confidential patient information) may be released to the respective site or provider.
- Data must only released to familiar, authorized personnel.

The Illinois Department of Public Health makes client level information available to local health departments and designated agencies for routine surveillance, partner services and linkage to care. Data for specific health care facilities or providers (including confidential patient information) may be released to the respective site/provider; however data MUST be released to familiar and authorized personnel at the specific facility. Under Illinois statutes, confidential information is never released to non-authorized individuals.



Data Release Decision Tree For Sharing and Releasing Non-Identifiable Data

1. Do any laws exist that prohibit release of requested data?

Yes: DO NOT Release Data

No:

2. Is this a routine request that adheres to cell size guidelines?

Yes: Release Data

No:

3. Does release of data clearly pass the IDPH Division of Infectious Disease (DID) Policy on release of Data Criteria?

Yes: Release Data

No:

4. Is the release of data for public health purposes

No: DO NOT Release Data

Yes:

5. Does the benefit of releasing data outweigh risk of potentially identifying a person?

Yes: Submit request to IDPH DID Release Expert for review

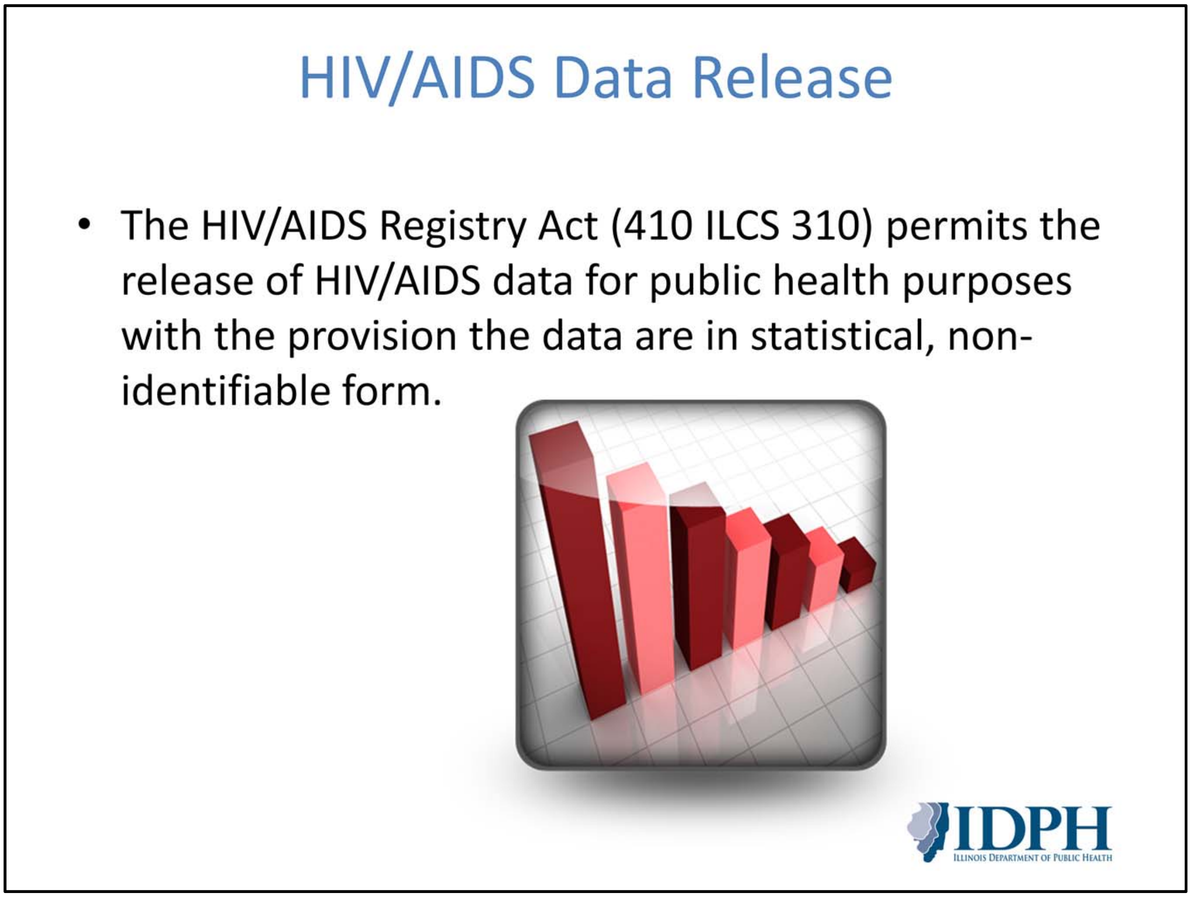
No: DO NOT Release Data

This slide will cover the data release decision tree for sharing and releasing non-identifiable data. This data release decision tree is a helpful tool to use when determining whether or not it is appropriate for you to share particular sets of data with outside entities. If ever in doubt, contact your agencies ORP or the applicable IDPH Section within the Office of Health Protection to help guide you on ***these decisions***.

The first question to ask yourself is, “Do any laws exist that prohibit the release of requested data?” If the answer is “Yes”, then do not release the data; If “No”, then ask yourself the next question, “Is this a routine request that adheres to cell size guidelines?” For HIV data, cell sizes cannot be less than 5 and not be censored. For communicable diseases and sexually transmitted disease data release, refer to the Division of Infectious Diseases Policy on Release of Communicable Disease Surveillance Data guidelines.

If the answer to the second question is “Yes”, then data may be released; otherwise if “No”, then ask the next question, “Does release of data clearly pass the IDPH Division of Infectious Disease or DID Policy on the release of Data Criteria.” If the answer is “Yes”, then data may be released; otherwise if “No” then ask the next question, “Is the release of data for public health purposes?”

If the answer is, “No”, then data may NOT be released; otherwise if “Yes”, then ask the next question, “Does the benefit of releasing data outweigh the risk of potentially identifying a person?” If the answer to this question is “No”, the data may NOT be released; otherwise, if “Yes” please submit a request to the IDPH DID Release Expert for review.

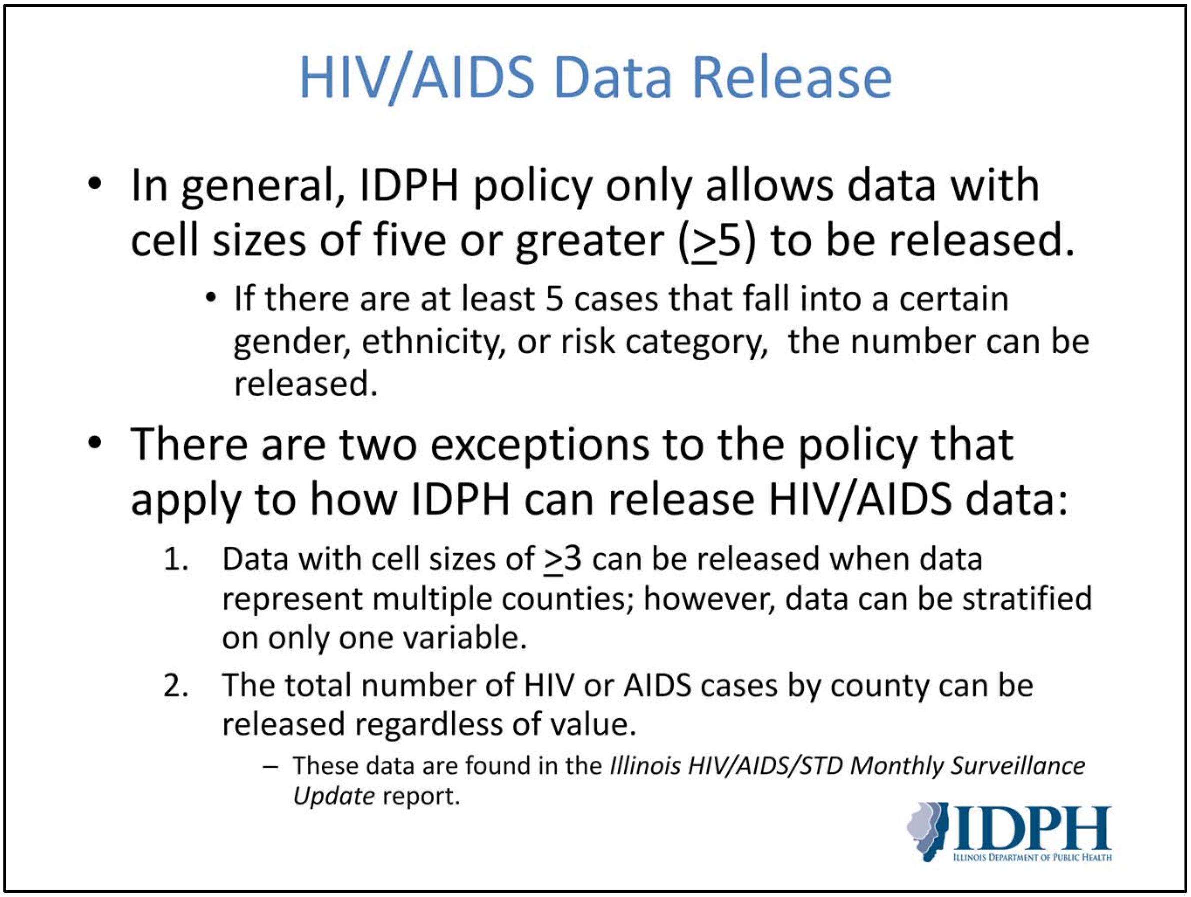


HIV/AIDS Data Release

- The HIV/AIDS Registry Act (410 ILCS 310) permits the release of HIV/AIDS data for public health purposes with the provision the data are in statistical, non-identifiable form.

IDPH
Illinois Department of Public Health

The release of HIV/AIDS data for public health purposes to non-HIV program staff is permitted as long as it is in statistical, non-identifiable format.



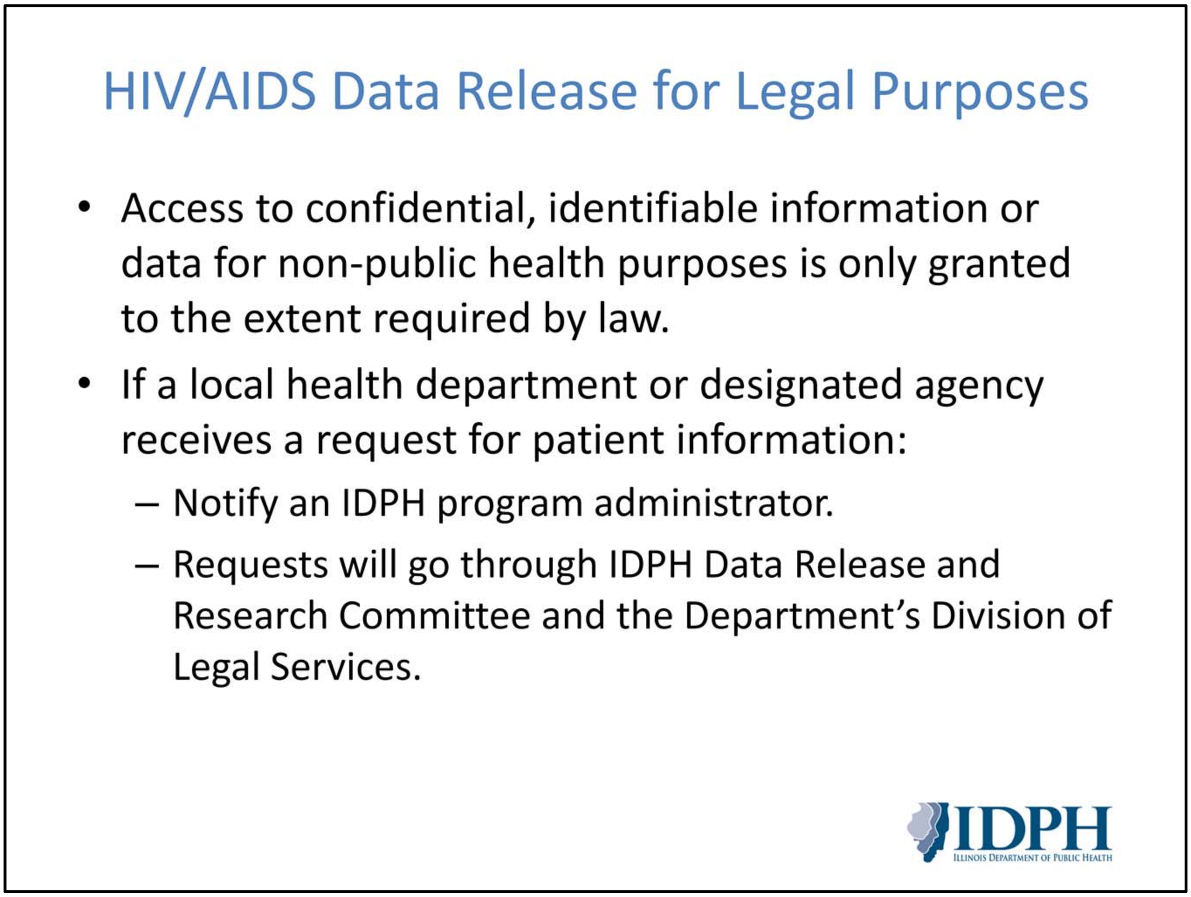
HIV/AIDS Data Release

- In general, IDPH policy only allows data with cell sizes of five or greater (≥5) to be released.
  - If there are at least 5 cases that fall into a certain gender, ethnicity, or risk category, the number can be released.
- There are two exceptions to the policy that apply to how IDPH can release HIV/AIDS data:
  1. Data with cell sizes of ≥3 can be released when data represent multiple counties; however, data can be stratified on only one variable.
  2. The total number of HIV or AIDS cases by county can be released regardless of value.
     - These data are found in the *Illinois HIV/AIDS/STD Monthly Surveillance Update* report.

In general, IDPH allows the release of data as long as cell sizes are a value of 5 or greater, that is, if there are at least five cases that fall into a certain gender, ethnicity, and risk category, the number of people falling into that category can be released. If there are 4 or fewer cases falling into the category, the number CANNOT be released. Jurisdictions with smaller populations of HIV cases are sometimes unable to report gender, ethnicity, and risk differences because of small cell sizes.

There are 2 exceptions to this policy, which apply to how IDPH can release the data it collects. These don't apply to how local jurisdictions can release data.
Exception #1: When data represents more than one county, it can be released if the number of cases is three or greater. However, data can only be stratified by 1 variable, such as risk, race, or gender.
Exception #2: The total number of HIV/AIDS cases by county can be released regardless of their value. But those data cannot be stratified on any variable other than County.

These data are found in the monthly surveillance update reports. And Local Health Departments are given updated county data each year that they can disseminate as long as the data release polices are followed.



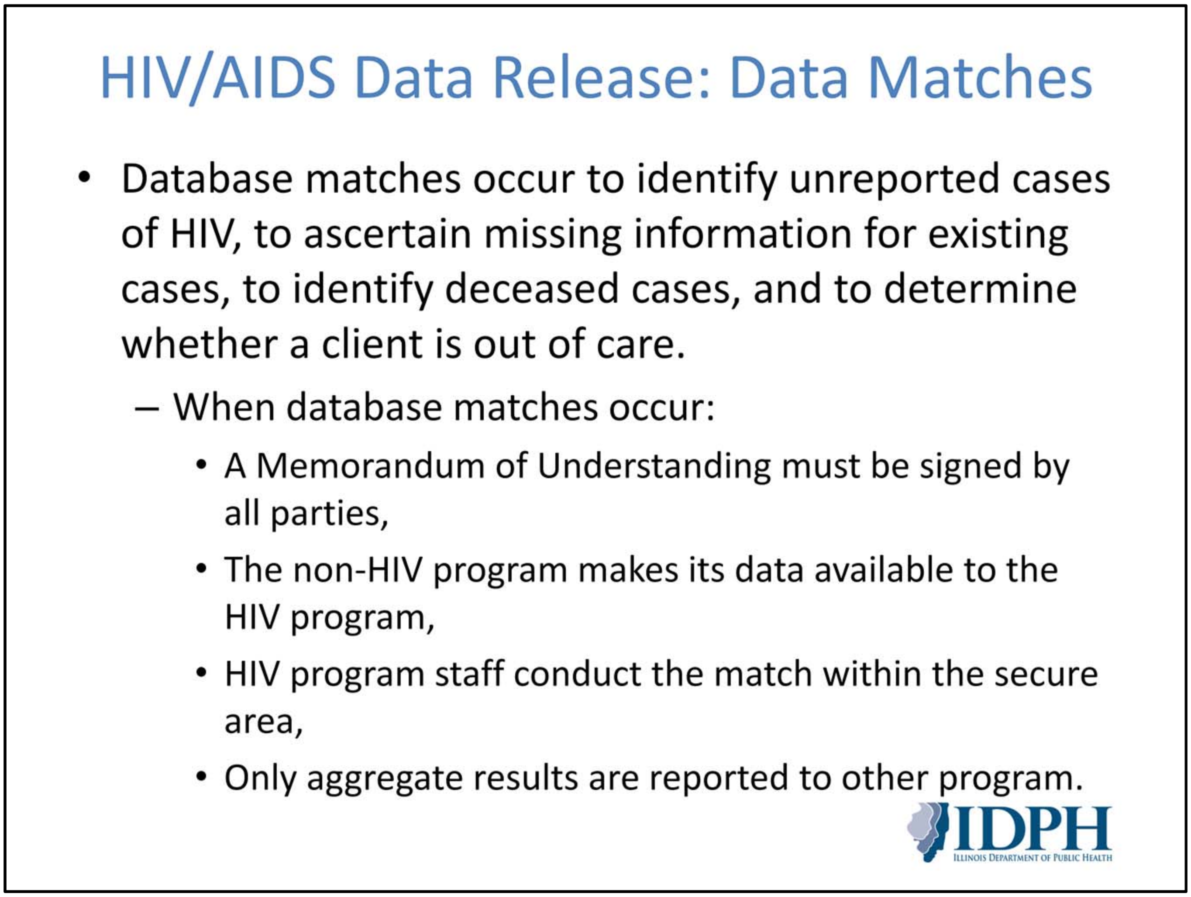
HIV/AIDS Data Release for Legal Purposes

- Access to confidential, identifiable information or data for non-public health purposes is only granted to the extent required by law.
- If a local health department or designated agency receives a request for patient information:
  – Notify an IDPH program administrator.
  – Requests will go through IDPH Data Release and Research Committee and the Department’s Division of Legal Services.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Access to confidential, identifiable HIV information or data maintained by IDPH or its designated agents for *non-public health purposes* is only granted to the extent required by law. This may include subpoenas or requests from attorneys on behalf of their client. If a local health department or designated agency receives a request for confidential patient information from unauthorized individuals or non HIV program staff, the request should be brought to the attention of the appropriate program administrator at the Illinois Department of Public Health, who would then alert the Data Release and Research Committee and the Department’s Division of Legal Services.

In such a case, the Illinois Department of Public Health HIV/AIDS Surveillance staff will:
-Obtain a signed request from the individual or legally authorized representative whose records are being requested and
-Indicate if such record exists
-If available, the information would be sent to the Department’s Division of Legal Services
-The Division of Legal Services would then release the information



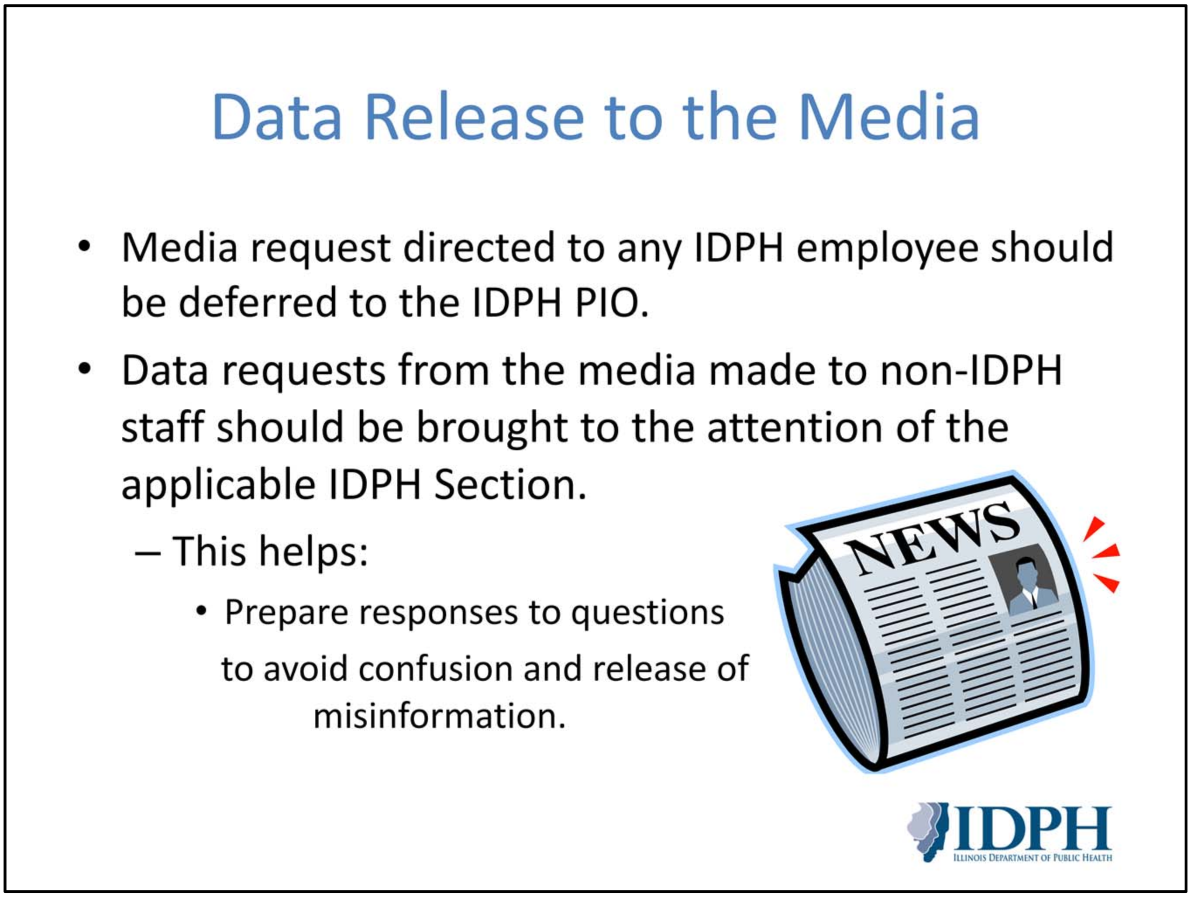
HIV/AIDS Data Release: Data Matches

- Database matches occur to identify unreported cases of HIV, to ascertain missing information for existing cases, to identify deceased cases, and to determine whether a client is out of care.
  - When database matches occur:
    - A Memorandum of Understanding must be signed by all parties,
    - The non-HIV program makes its data available to the HIV program,
    - HIV program staff conduct the match within the secure area,
    - Only aggregate results are reported to other program.

IDPH
Illinois Department of Public Health

The Illinois Department of Public Health often conducts data matches to identify unreported cases of HIV, to ascertain missing information for existing cases, to identify deceased cases and to determine whether a client is out of care. The IDPH HIV Surveillance office shares and receives information with other programs within the HIV/AIDS section (such as Counseling/Testing, AIDS Drug Assistance Program (or ADAP), Prevention, and Partner Services) as well as other programs outside the HIV section (such as Vital Records, TB, and STD sections).

When these data matches occur:
-A Memorandum of Understanding must be signed by all parties
-The non-HIV program Surveillance makes its data available to the HIV program, meaning the non-HIV program gives information to the HIV program, and the HIV program conducts the search within the secure HIV Surveillance area.
-After the match or search is conducted, the HIV program staff reports its findings back to the non-HIV program
-Only aggregate results are reported to other program.



Data Release to the Media

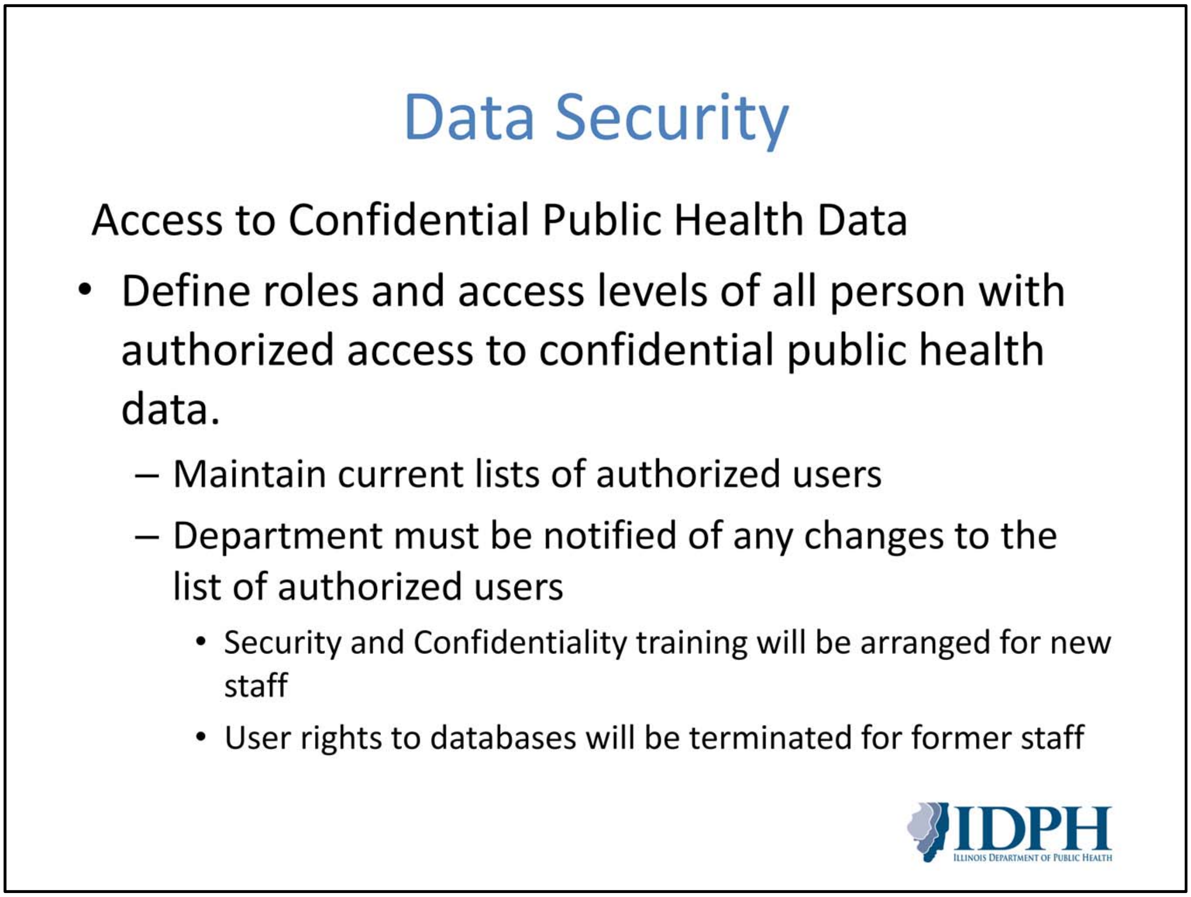
- Media request directed to any IDPH employee should be deferred to the IDPH PIO.
- Data requests from the media made to non-IDPH staff should be brought to the attention of the applicable IDPH Section.
  - This helps:
    - Prepare responses to questions to avoid confusion and release of misinformation.

Requests from the media directed to any IDPH employee should be deferred to the IDPH Public Information Officer or the PIO. If specific data or information is needed, the PIO will contact the appropriate IDPH Section and return responses to the media.

As a courtesy, IDPH asks that data requests from the media made to non-IDPH staff should be brought to the attention of the applicable IDPH Section. This can help prepare IDPH with responses to follow-up questions from the media and can avoid confusion or the release of misinformation.

DATA SECURITY

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

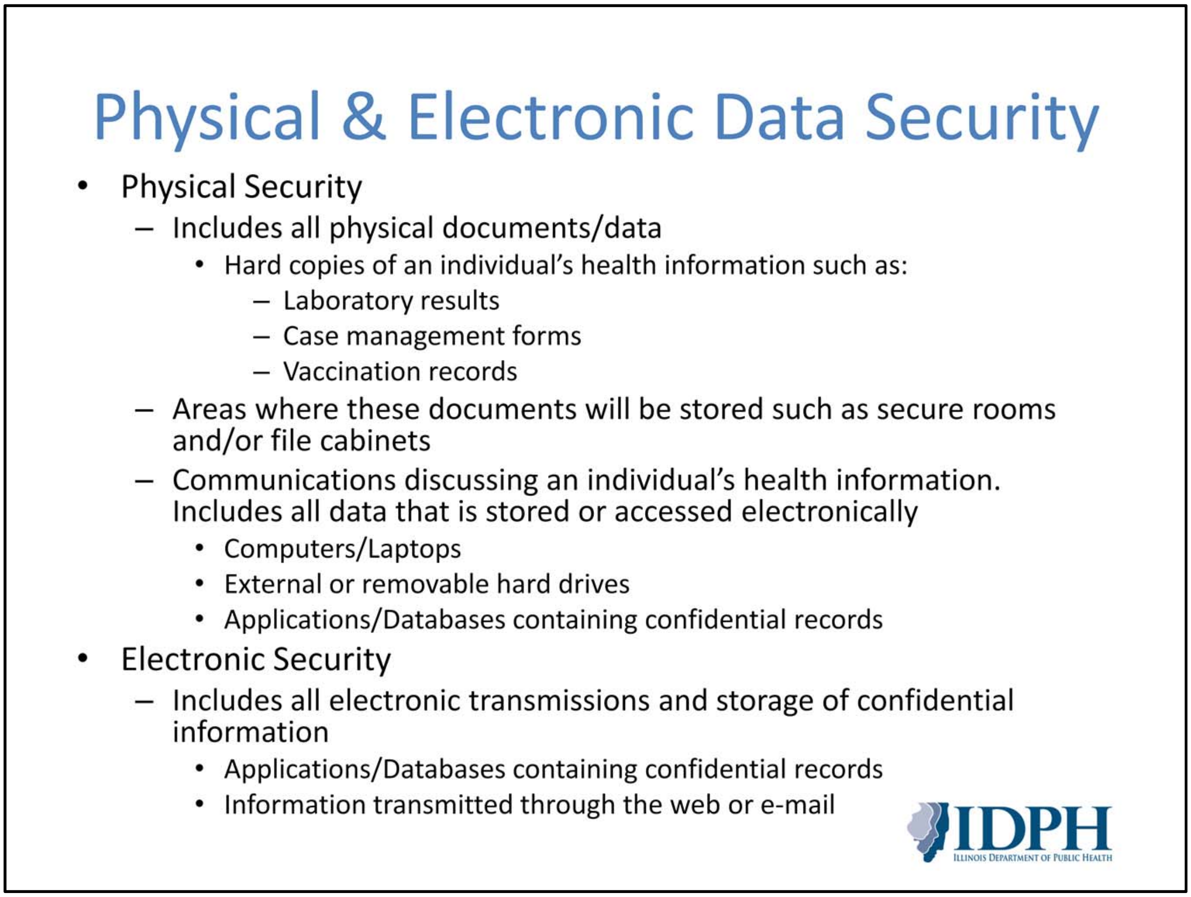


Data Security

Access to Confidential Public Health Data

- Define roles and access levels of all person with authorized access to confidential public health data.
  - Maintain current lists of authorized users
  - Department must be notified of any changes to the list of authorized users
    - Security and Confidentiality training will be arranged for new staff
    - User rights to databases will be terminated for former staff

At all agencies that follow these security and confidentiality guidelines, staff who have access to confidential public health data should have their roles defined and only those staff should have the necessary authorized access to confidential public health data. A list of current authorized users should be maintained. IDPH must be notified of any changes to the list of authorized users (such as when new users need access and when users leaves their agencies). Security and Confidentiality training will be arranged for new staff and user rights to databases will be terminated for former staff.



Physical & Electronic Data Security

- Physical Security
  - Includes all physical documents/data
    - Hard copies of an individual’s health information such as:
      - Laboratory results
      - Case management forms
      - Vaccination records
  - Areas where these documents will be stored such as secure rooms and/or file cabinets
  - Communications discussing an individual’s health information. Includes all data that is stored or accessed electronically
    - Computers/Laptops
    - External or removable hard drives
    - Applications/Databases containing confidential records
- Electronic Security
  - Includes all electronic transmissions and storage of confidential information
    - Applications/Databases containing confidential records
    - Information transmitted through the web or e-mail

IDPH
Illinois Department of Public Health

In the next few slides, we will be discussing the two types of data security: physical and electronic. Physical Security includes all physical documents or data. For example, hard copies of an individual’s health information such as: laboratory results, case management forms, or vaccination records. Physical Security also includes areas where these documents will be stored such as secure rooms, file cabinets, computers, laptops, and external or removable hard drives; as well as any communications discussing an individual’s health information such as memos and reports.

Electronic Security includes all electronic transmissions and storage of confidential information. This includes application and database storage of confidential data (such as STI surveillance systems, registries, and databases on servers) and electronic transmissions (such as transmissions over the web or e-mails).

Physical & Electronic Data Security

Physical Security

Electronic Data Security

Patient's Laboratory Results

Creatinine 2.2 mg/dl
eGFR 34 ml/min per 1.73 m² → CKD Stage 3

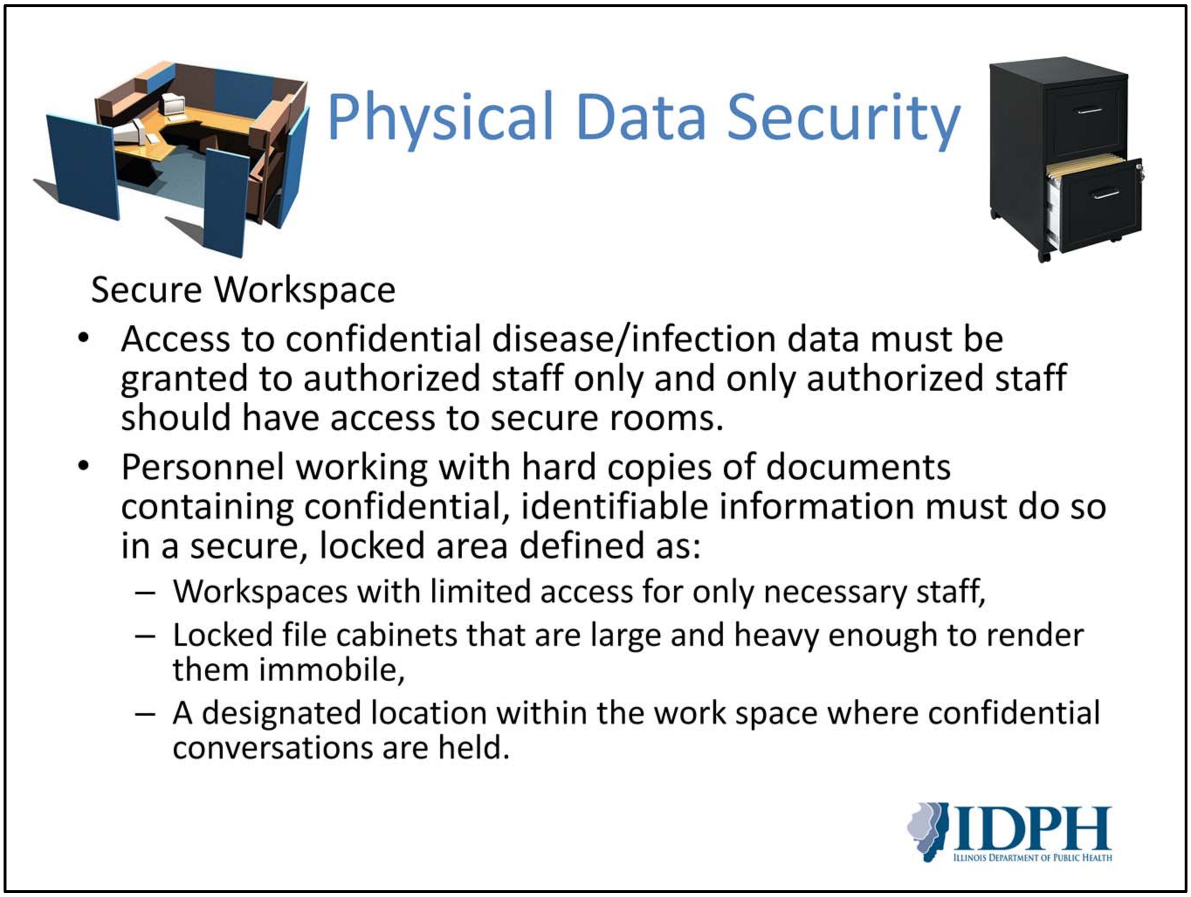
Na⁺	140	mEq/L	Ca⁺⁺	8.6	mg/dl
K⁺	4.8	mEq/L	HPO₄⁻	5.2	mg/dl
Cl⁻	105	mEq/L	Albumin	3.6	mg/dl
HCO₃⁻	20	mEq/L	PTH	150	pg/ml
Hg	10.5	g/dl			

IDPH
Illinois Department of Public Health

Here are some examples of physical and electronic data security items.

Physical data securities on items in the physical work environment like cubicles, work stations, or storage devices like file cabinets; Lab results and reporting forms
Electronic hardware like laptops, hard drives, flash drives, and other portable devices.

Electronic data securities need to cover items like data servers, electronic data transmissions, and e-mails.



Physical Data Security

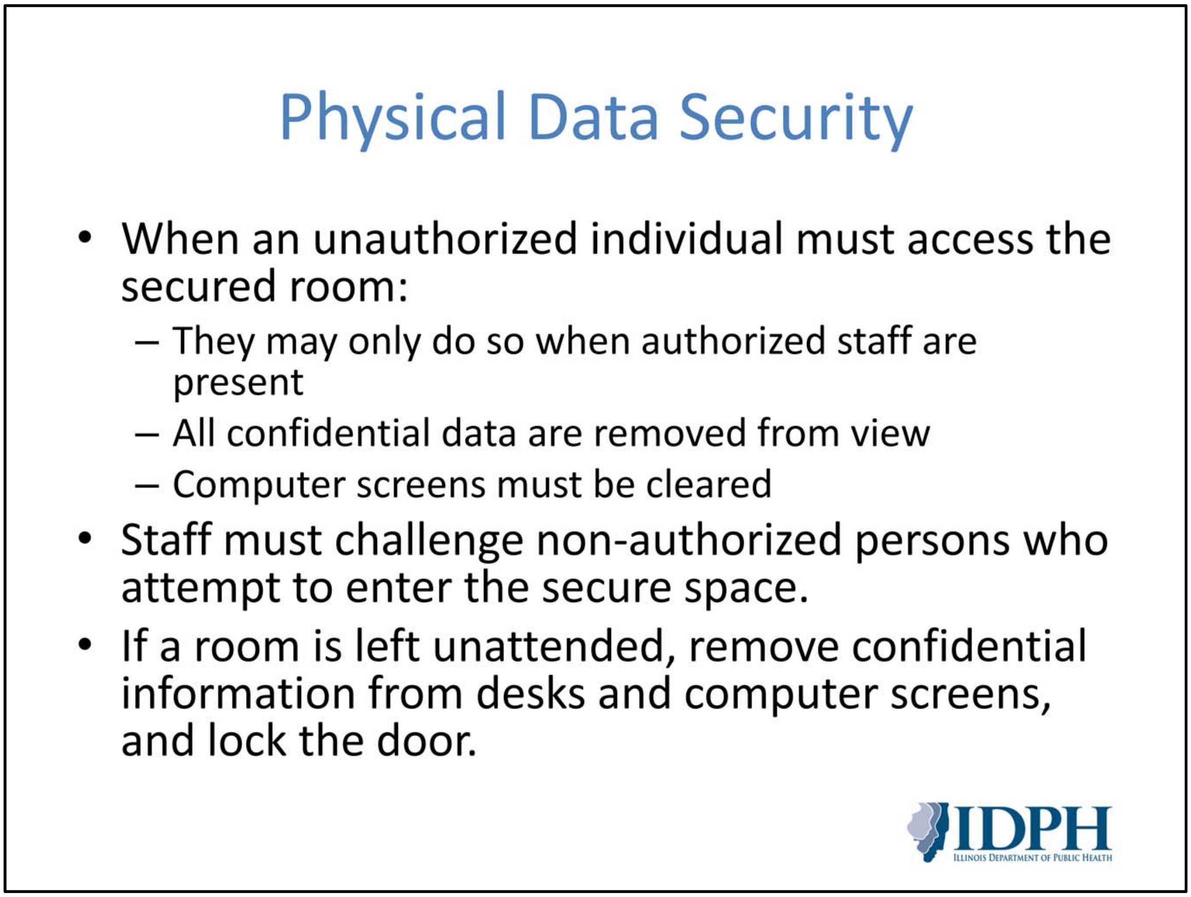
Secure Workspace

- Access to confidential disease/infection data must be granted to authorized staff only and only authorized staff should have access to secure rooms.
- Personnel working with hard copies of documents containing confidential, identifiable information must do so in a secure, locked area defined as:
  - Workspaces with limited access for only necessary staff,
  - Locked file cabinets that are large and heavy enough to render them immobile,
  - A designated location within the work space where confidential conversations are held.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Access to confidential disease/infection data must be granted to authorized staff only and only authorized staff should have access to secure rooms where this data is stored.
Personnel working with documents containing confidential, identifiable information must do so in a secure, locked area. The secure area should include:
A workspace with limited access for only necessary, authorized staff;
Locked file cabinets that are not easily moveable; and
A designated location within the work space where confidential conversations are held.

Discussions about anything confidential should not take place in the vicinity of unauthorized persons.



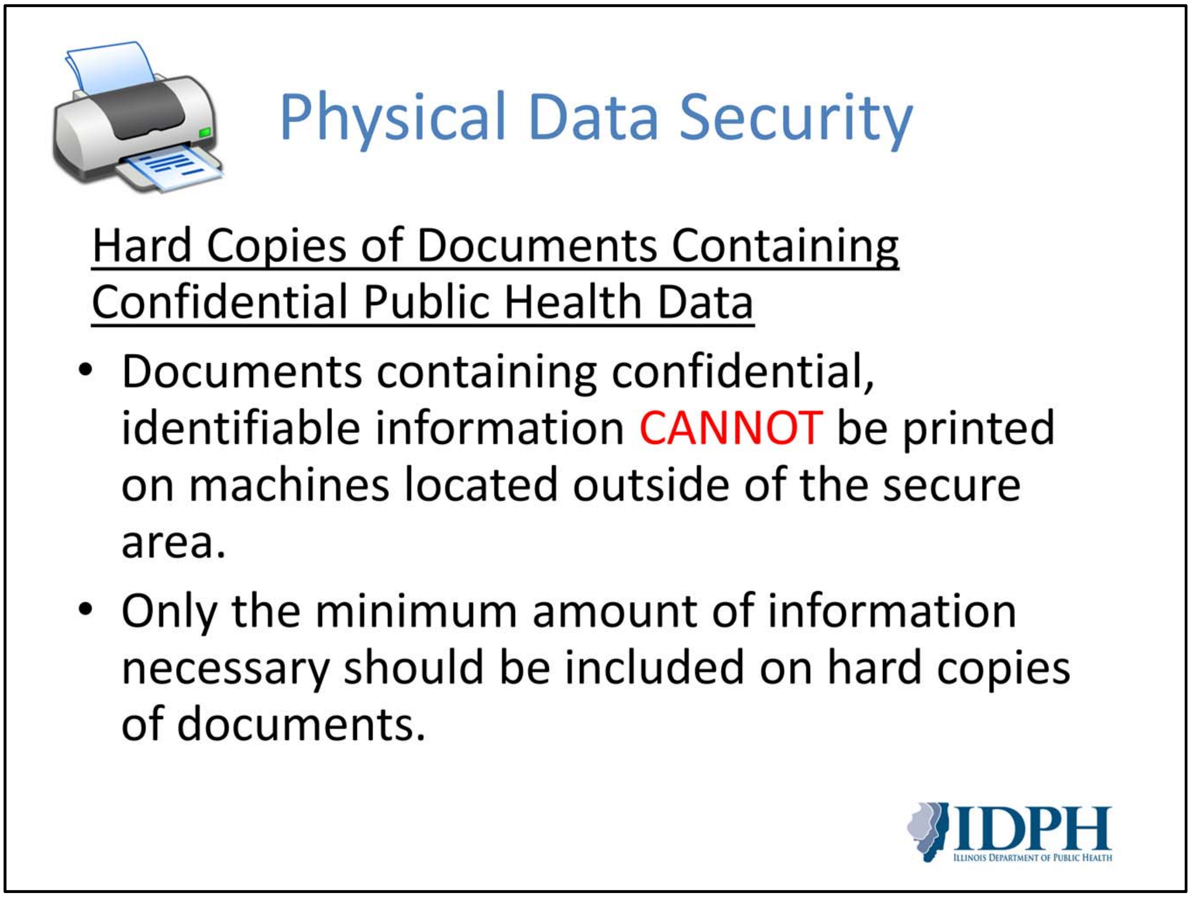
Physical Data Security

- When an unauthorized individual must access the secured room:
  - They may only do so when authorized staff are present
  - All confidential data are removed from view
  - Computer screens must be cleared
- Staff must challenge non-authorized persons who attempt to enter the secure space.
- If a room is left unattended, remove confidential information from desks and computer screens, and lock the door.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Only authorized staff should have access and keys to secure rooms and doors should be locked when unattended. When unauthorized personnel such as building maintenance, repair crew, etc must enter a restricted workspace: At least one authorized staff must be present, all confidential information must be removed from view, and computer screens must be cleared of confidential information.

Staff should challenge non-authorized persons who attempt to enter a secured room to make sure they have a reason to be in the room. If there is a need for an unauthorized individual to have access to a secured room, it should be only when there is an absolute need to do so. For example, a building cleaning or repair crew working on tasks. Doors to secure rooms must be locked when unattended. If you have to leave your desk, even if just for a moment, you must remove confidential information from your desk and computer screen and lock the office door.



Physical Data Security

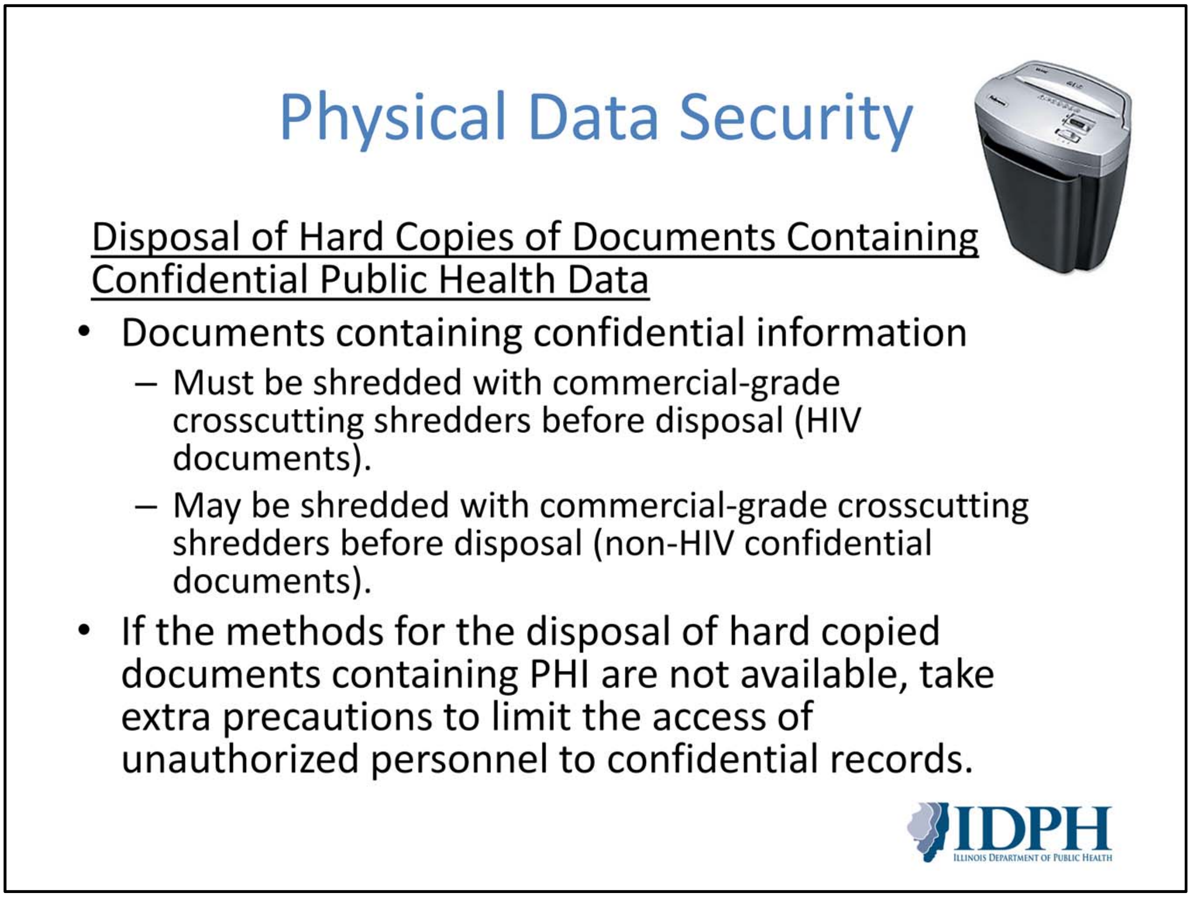
Hard Copies of Documents Containing Confidential Public Health Data

- Documents containing confidential, identifiable information CANNOT be printed on machines located outside of the secure area.
- Only the minimum amount of information necessary should be included on hard copies of documents.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When printing documents containing confidential information whenever possible, printers should be located within the secure area and should not be printed on machines outside of the area.

If a printer is not available within a secure room, take extra precautions to limit the access of unauthorized personnel to confidential records. For example, have another authorized staff person go to the printer where the print job is being sent before printing a document, so that the authorized staff member can take the print job immediately from the printer, therein reducing the likelihood that an unauthorized person would accidentally intercept the print job. Only the minimum amount of information necessary should be included on hard copies of documents, so be mindful when printing confidential information.



Physical Data Security

Disposal of Hard Copies of Documents Containing Confidential Public Health Data

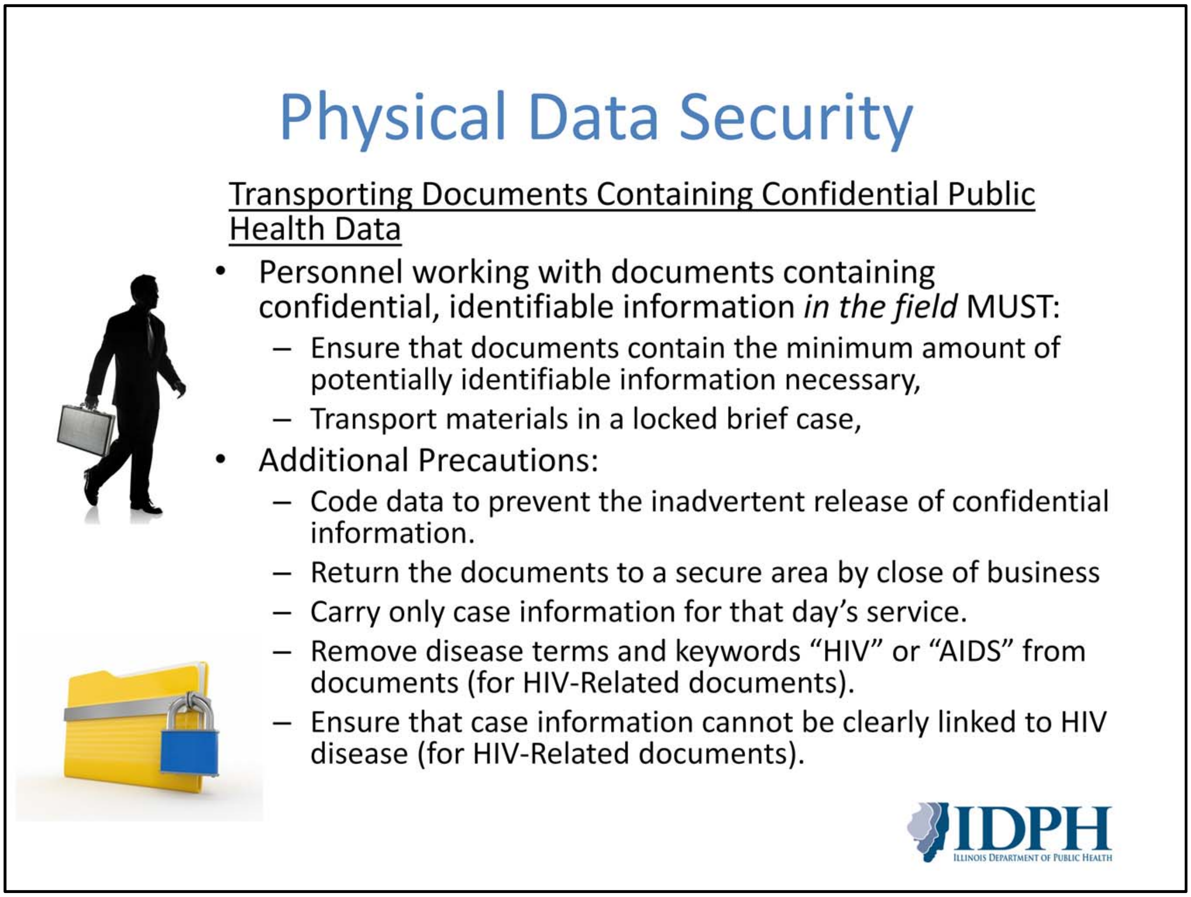
- Documents containing confidential information
  - Must be shredded with commercial-grade crosscutting shredders before disposal (HIV documents).
  - May be shredded with commercial-grade crosscutting shredders before disposal (non-HIV confidential documents).
- If the methods for the disposal of hard copied documents containing PHI are not available, take extra precautions to limit the access of unauthorized personnel to confidential records.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When disposing documents containing confidential information, a commercial-grade crosscutting shredder should be used prior to disposal. **For HIV Programs, crosscutting shredders are required.**

Whenever possible, shredders should be located within the secure area. If a cross-cutting shredder is not available within a secure room, shredding can take place outside of the secure room as long as the authorized staff person takes extra caution to minimize the chance of unauthorized staff seeing confidential information. If it is a small shredding job, the staff could black out all of the names; or if it is a large job, make sure that all the paperwork is facing down to prevent exposing confidential information.

If the methods for the disposal of hard copied documents containing PHI are not available, take extra precautions to limit the access of unauthorized personnel to confidential records.



Physical Data Security

Transporting Documents Containing Confidential Public Health Data

- Personnel working with documents containing confidential, identifiable information *in the field* MUST:
  - Ensure that documents contain the minimum amount of potentially identifiable information necessary,
  - Transport materials in a locked brief case,
- Additional Precautions:
  - Code data to prevent the inadvertent release of confidential information.
  - Return the documents to a secure area by close of business
  - Carry only case information for that day’s service.
  - Remove disease terms and keywords “HIV” or “AIDS” from documents (for HIV-Related documents).
  - Ensure that case information cannot be clearly linked to HIV disease (for HIV-Related documents).

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

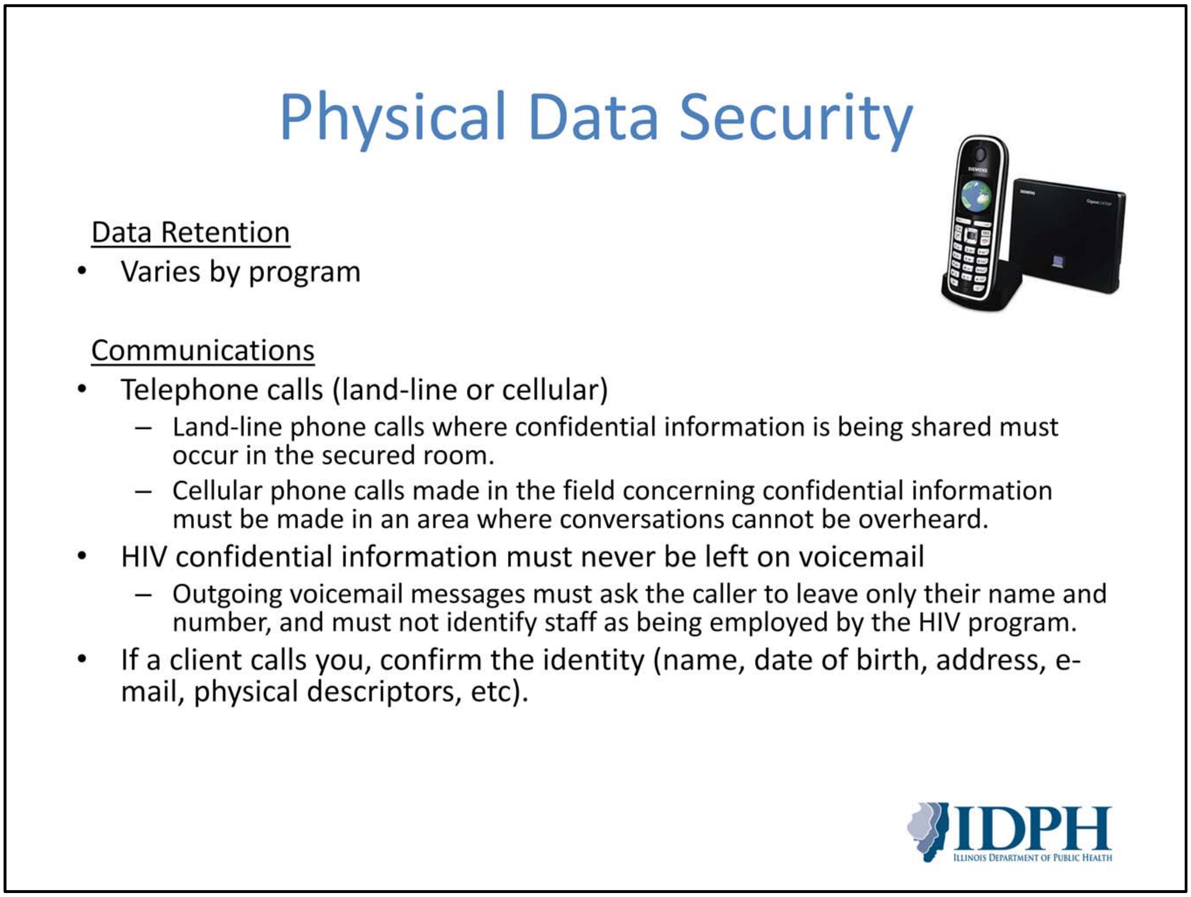
When confidential health information is taken into the field, personnel working with documents containing confidential, identifiable information must:
Ensure that documents contain the minimum amount of potentially identifiable information necessary.
Transport materials in a locked briefcase. The lock combination and/or keys may only be shared with authorized staff.

As additional precautions, staff should also:

- Code data using a state number or client code in order to prevent the inadvertent release of confidential information.
- Return the documents to a secure area by close of business. If it’s not possible to return to the office the same day, staff should receive prior approval from a supervisor to hold on to the information until it’s possible to return to the office. Any confidential information kept overnight must remain inside the locked brief case and be taken into private residence, then returned as soon as possible.
- Carry only case information for that day’s service. Completed forms must be placed in sealed envelopes.
- Remove any key disease/infection terms such as “HIV”, “AIDS”, “Syphilis”, or any other disease specific terms from documents. For example, terms such as CD4 or Viral Load could link a person to HIV infection.

- Ensure that case information cannot be clearly linked to HIV disease. Any forms completed must not contain patient names (only codes) ***and*** no un-coded references to HIV disease terminology.

It is also a good idea to carry pamphlet and referral information separately from the patient information, and to carry pre-addressed, stamped, and double envelopes marked “Confidential” and “To Addressee Only” should you need to mail sensitive information.



Physical Data Security

Data Retention

- Varies by program

Communications

- Telephone calls (land-line or cellular)
  - Land-line phone calls where confidential information is being shared must occur in the secured room.
  - Cellular phone calls made in the field concerning confidential information must be made in an area where conversations cannot be overheard.
- HIV confidential information must never be left on voicemail
  - Outgoing voicemail messages must ask the caller to leave only their name and number, and must not identify staff as being employed by the HIV program.
- If a client calls you, confirm the identity (name, date of birth, address, e-mail, physical descriptors, etc).

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

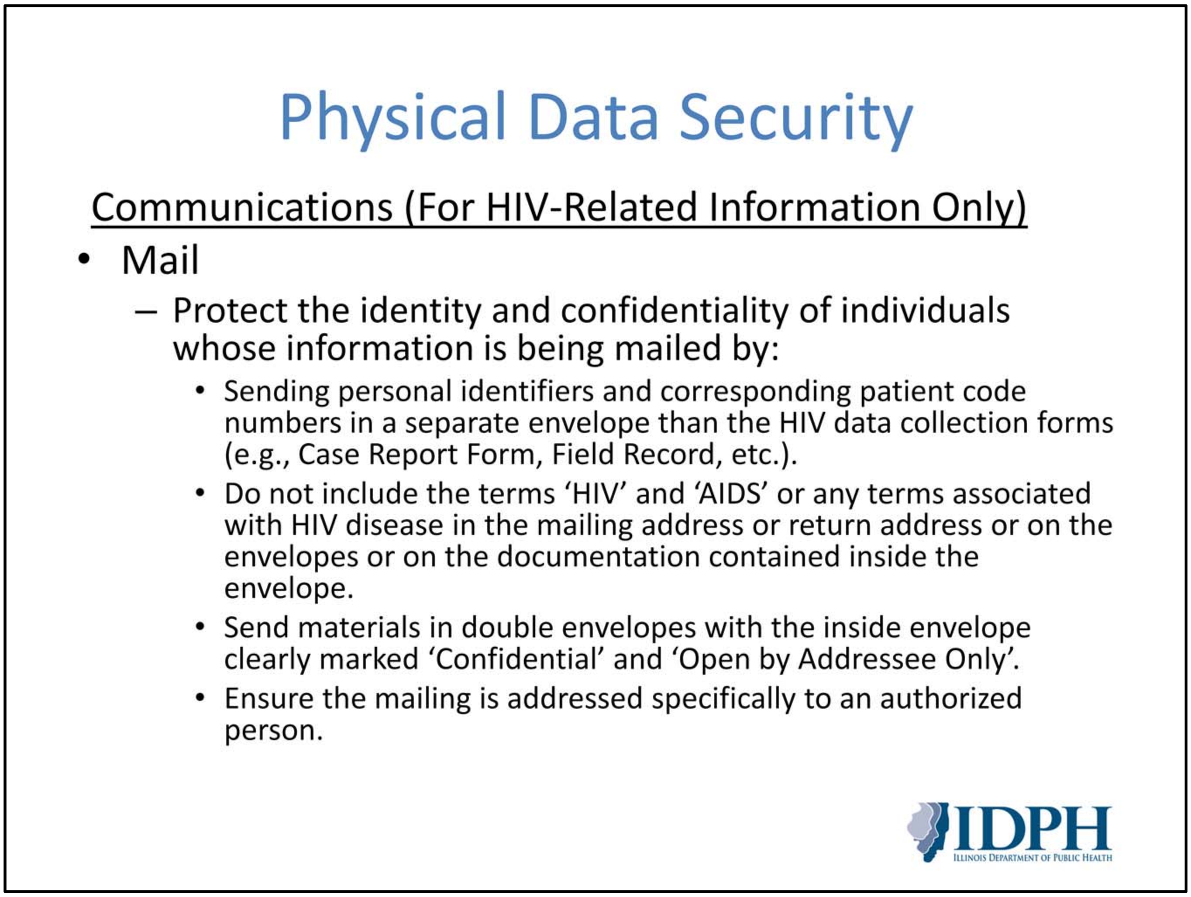
The retention of data and confidential records varies by program. **All confidential records and data shall be stored in secure rooms and in locked cabinets.**

Land-line and cellular phone calls, whether in the office or out in the field, that share confidential information must occur in a secure area where conversations cannot be overheard.

HIV confidential information must ***never*** be left on any voicemail. Outgoing voicemail messages must ask the caller to leave only their name and number, and must not identify staff as being employed by the **HIV** program. Even if a voice mailbox is only checked by one staff person, there is no way to guarantee that no one else will be able to gain access to voicemail messages. Outgoing voicemail messages should state "Please do not leave any confidential information on this voicemail." And ask the caller to leave only their name and phone number.

When calling a client and leaving voicemail, don't go into an explanation for your call or mention anything related to **any specific infection**, including identifying oneself from any particular disease program such as HIV, STD, or CD staff, for example. Simply state that you have important information that you need to speak about as soon as possible, and to please contact you back.

If a client calls you, confirm the identity by verifying the person’s name, date of birth, address, e-mail, physical descriptors, or any other identifiers available.



Physical Data Security

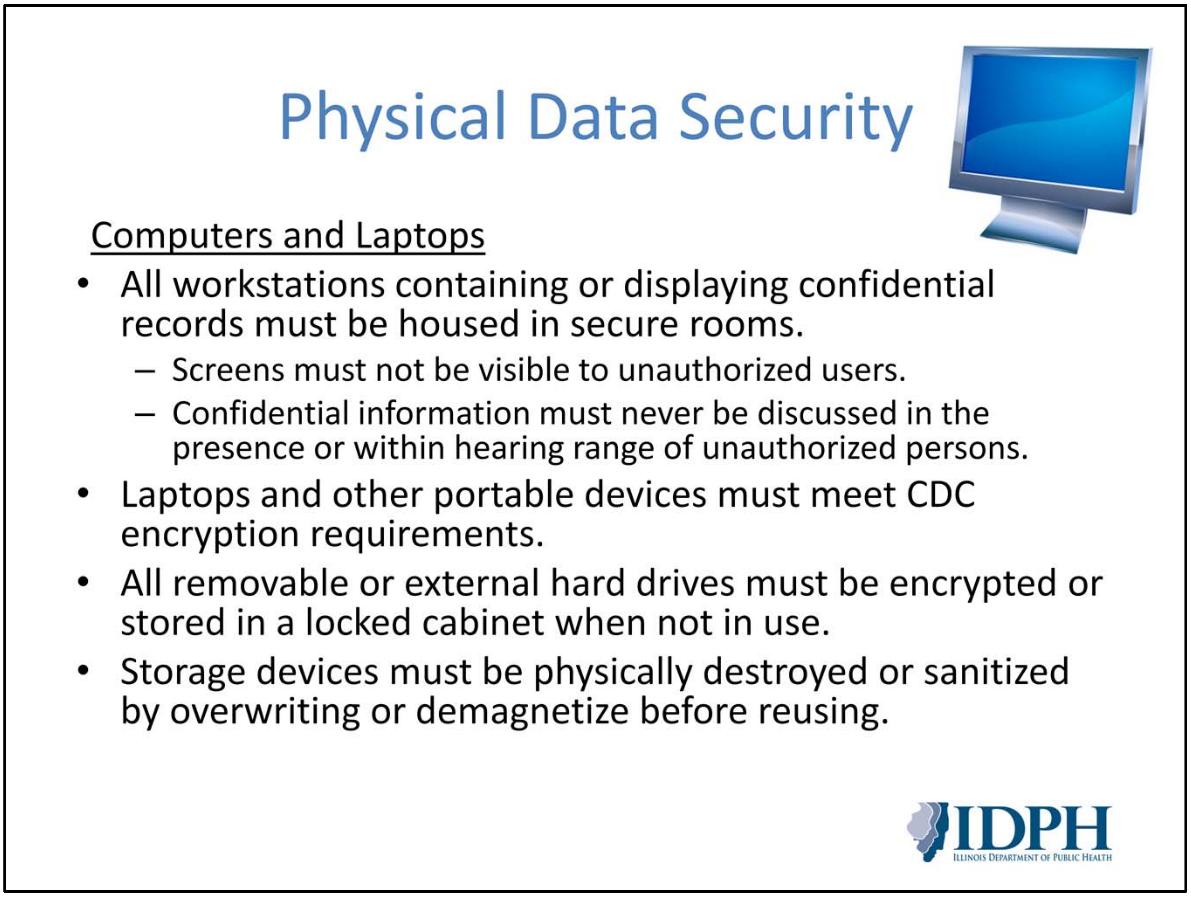
Communications (For HIV-Related Information Only)

- Mail
  - Protect the identity and confidentiality of individuals whose information is being mailed by:
    - Sending personal identifiers and corresponding patient code numbers in a separate envelope than the HIV data collection forms (e.g., Case Report Form, Field Record, etc.).
    - Do not include the terms ‘HIV’ and ‘AIDS’ or any terms associated with HIV disease in the mailing address or return address or on the envelopes or on the documentation contained inside the envelope.
    - Send materials in double envelopes with the inside envelope clearly marked ‘Confidential’ and ‘Open by Addressee Only’.
    - Ensure the mailing is addressed specifically to an authorized person.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When mailing sensitive or confidential HIV information, in order to protect the identity of individuals whose information is being mailed one should do the following:

- Send a patient’s personal identifiers and corresponding patient code numbers in a separate mailing than the HIV data collection forms. For example, a case report form that contains the patient’s HIV information should not include the patient’s name; rather, the form should only include a state number or other code number. The name and additional identifying information such as address and phone number with the corresponding code number should be sent separately in another envelope in order to link the patient to the case report. This way if one of the envelopes ends up in the wrong hands, the person who opens the envelope would not have the full confidential information regarding this patient. Either they would be able to see the name without the confidential HIV information, or the confidential HIV information but no name.
- Do not include the terms HIV or AIDS on the envelope, either in the mailing or return address, or on the documentation contained inside the envelope.
- Send materials in a double envelope, with the inside envelope marked “Confidential” and “Open by Addressee only.”
- Address the mailing to a specific authorized person as the intended recipient.



Physical Data Security

Computers and Laptops

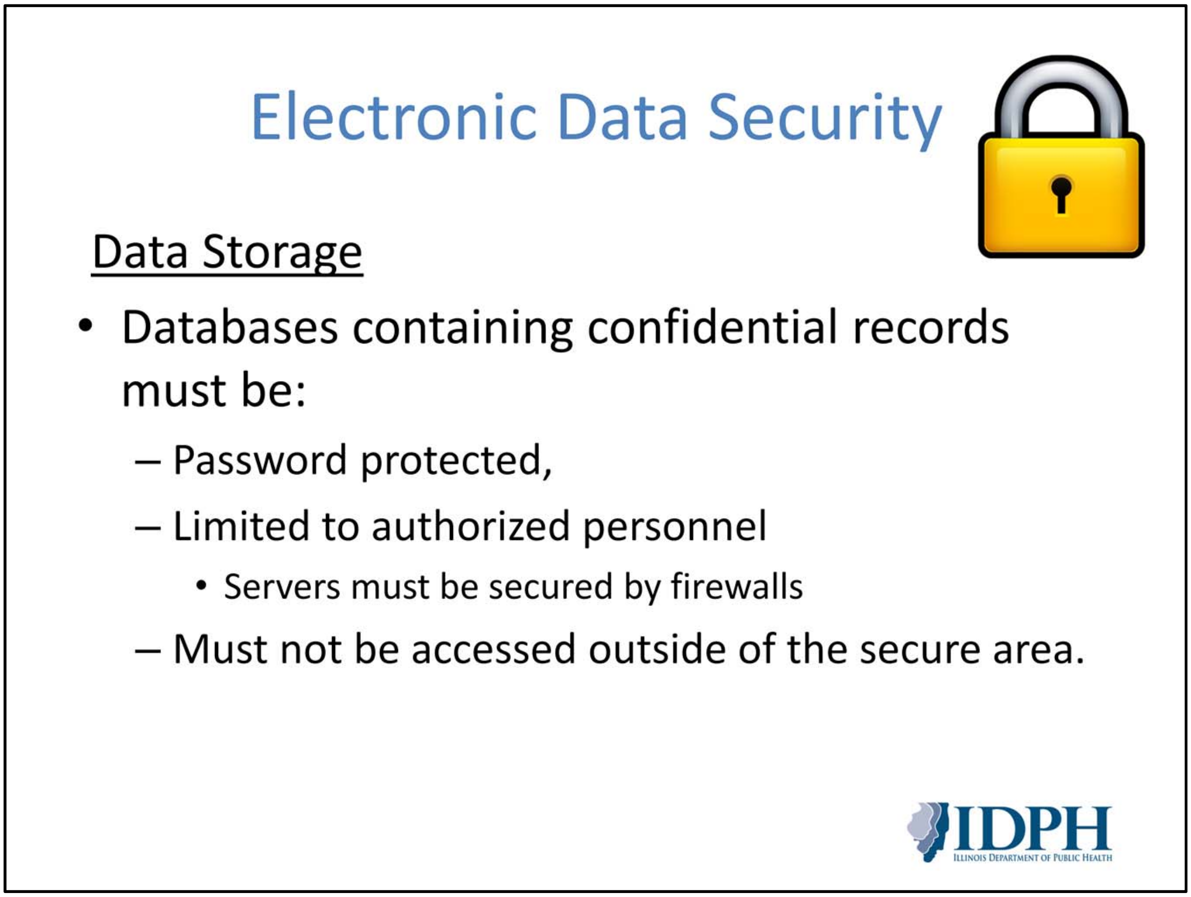
- All workstations containing or displaying confidential records must be housed in secure rooms.
  - Screens must not be visible to unauthorized users.
  - Confidential information must never be discussed in the presence or within hearing range of unauthorized persons.
- Laptops and other portable devices must meet CDC encryption requirements.
- All removable or external hard drives must be encrypted or stored in a locked cabinet when not in use.
- Storage devices must be physically destroyed or sanitized by overwriting or demagnetize before reusing.

IDPH
Illinois Department of Public Health

All workstations containing or displaying confidential records must be housed in secure rooms. Screens must not be visible to unauthorized users and confidential information must never be discussed in the presence or within hearing range of unauthorized persons.

Laptops, external hard drives, flash drives, and other portable devices must be encrypted and password protected and stored in either secure rooms and/or a locked cabinet when not in use.

Storage devices must be physically destroyed or sanitized by overwriting or demagnetizing before reusing.



Electronic Data Security

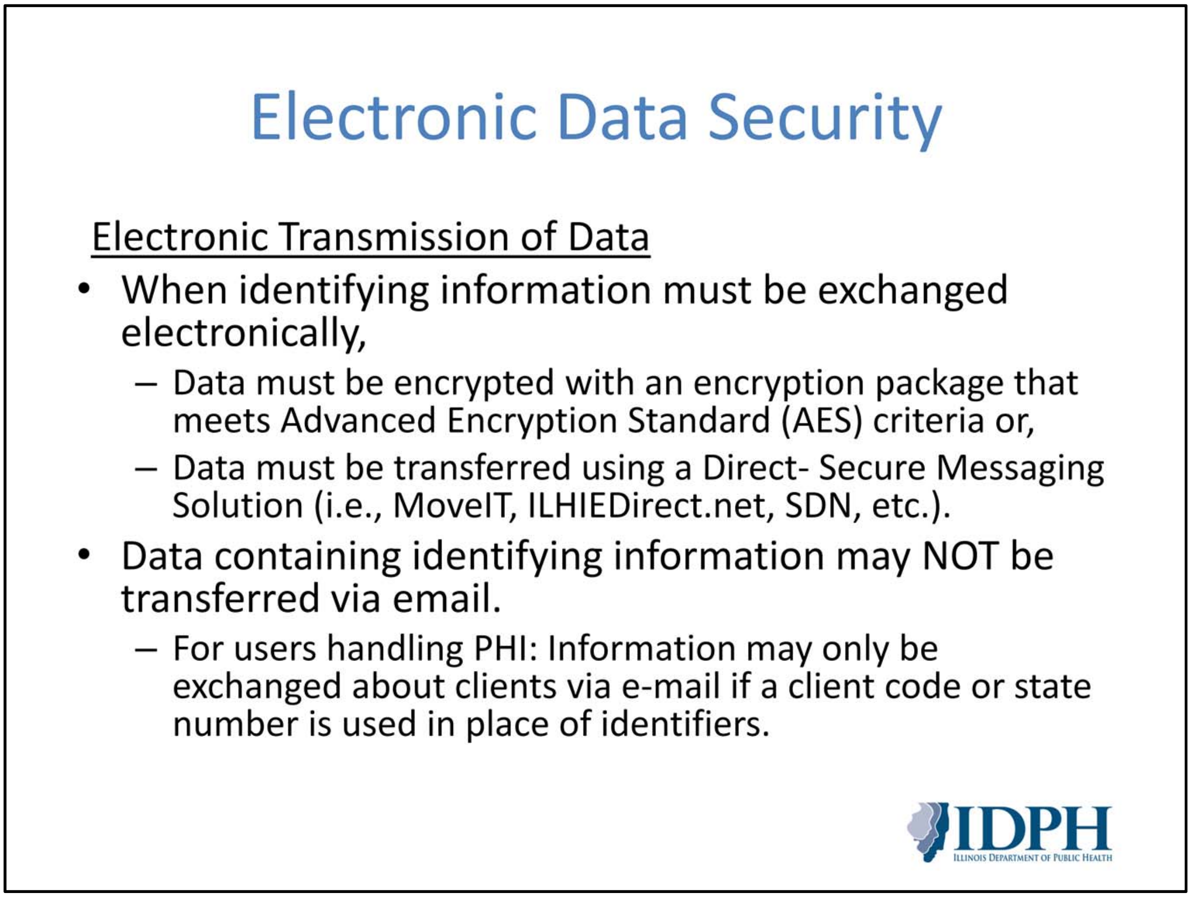
Data Storage

- Databases containing confidential records must be:
  - Password protected,
  - Limited to authorized personnel
    - Servers must be secured by firewalls
  - Must not be accessed outside of the secure area.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Databases or software systems with confidential records such as INEDSS, HIV Registries such as eHARS or Provide, and locally maintained systems must be password protected, located on servers or machines with limited access to authorized personnel and network administrators, and only be accessed within secure areas.

Staff are individually responsible for protecting their own work station, laptop, or other devices associated with confidential data, including keys and passwords, and to prevent damage to hardware or software.



Electronic Data Security

Electronic Transmission of Data

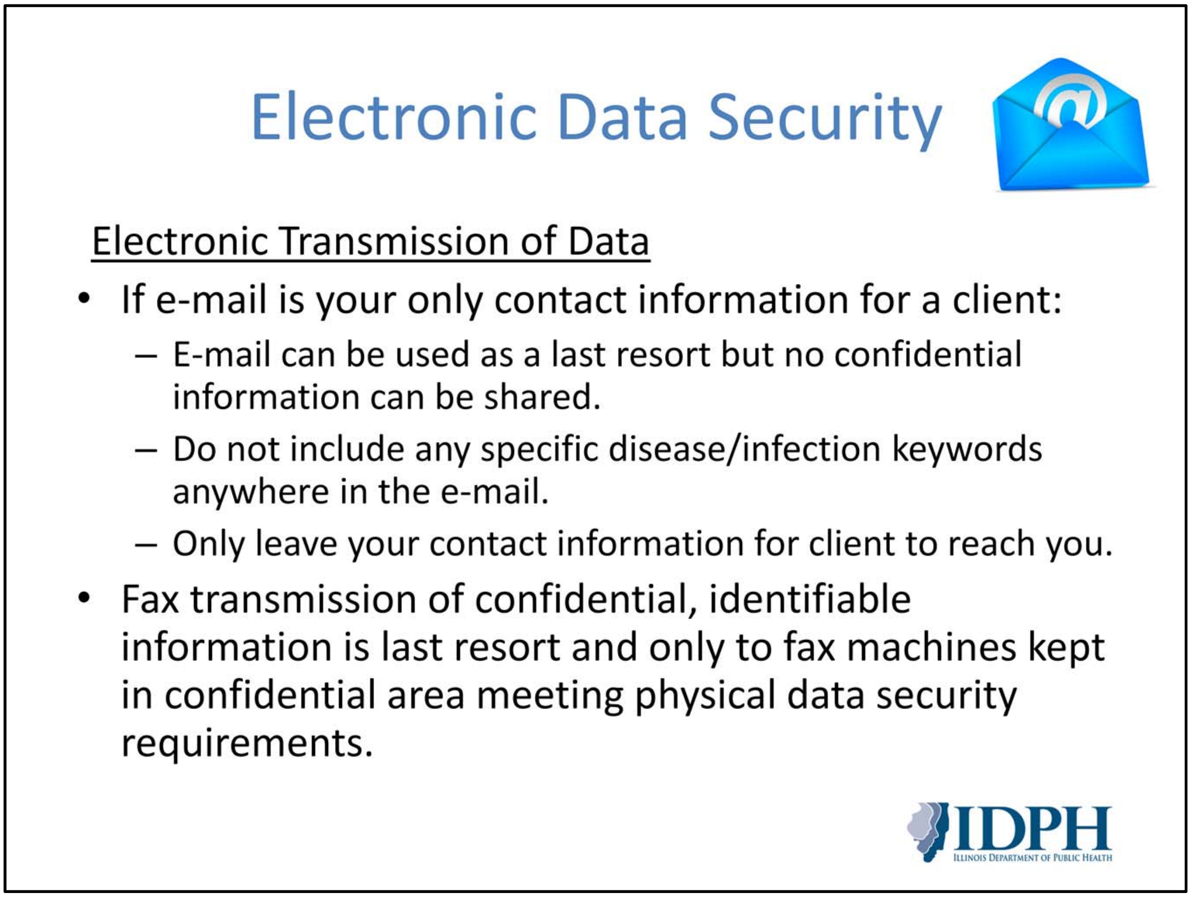
- When identifying information must be exchanged electronically,
  - Data must be encrypted with an encryption package that meets Advanced Encryption Standard (AES) criteria or,
  - Data must be transferred using a Direct- Secure Messaging Solution (i.e., MoveIT, ILHIEDirect.net, SDN, etc.).
- Data containing identifying information may NOT be transferred via email.
  - For users handling PHI: Information may only be exchanged about clients via e-mail if a client code or state number is used in place of identifiers.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

When identifying information must be exchanged electronically:

- data must be encrypted with an encryption package that meets Advanced Encryption Standard criteria, or
- data must be transferred using a Direct- Secure Messaging Solution or secure FTP.

Data containing identifying information may NOT be transferred via email. Identifying information such as client names, contact information, or lab info, may NEVER be e-mailed, either in the body of the e-mail or as an attachment, including line listings. However, information about clients CAN be exchanged using codes, such as the individual’s state number or client code provided the codes cannot include any identifiers, including gender and date of birth.



Electronic Data Security

Electronic Transmission of Data

- If e-mail is your only contact information for a client:
  - E-mail can be used as a last resort but no confidential information can be shared.
  - Do not include any specific disease/infection keywords anywhere in the e-mail.
  - Only leave your contact information for client to reach you.
- Fax transmission of confidential, identifiable information is last resort and only to fax machines kept in confidential area meeting physical data security requirements.

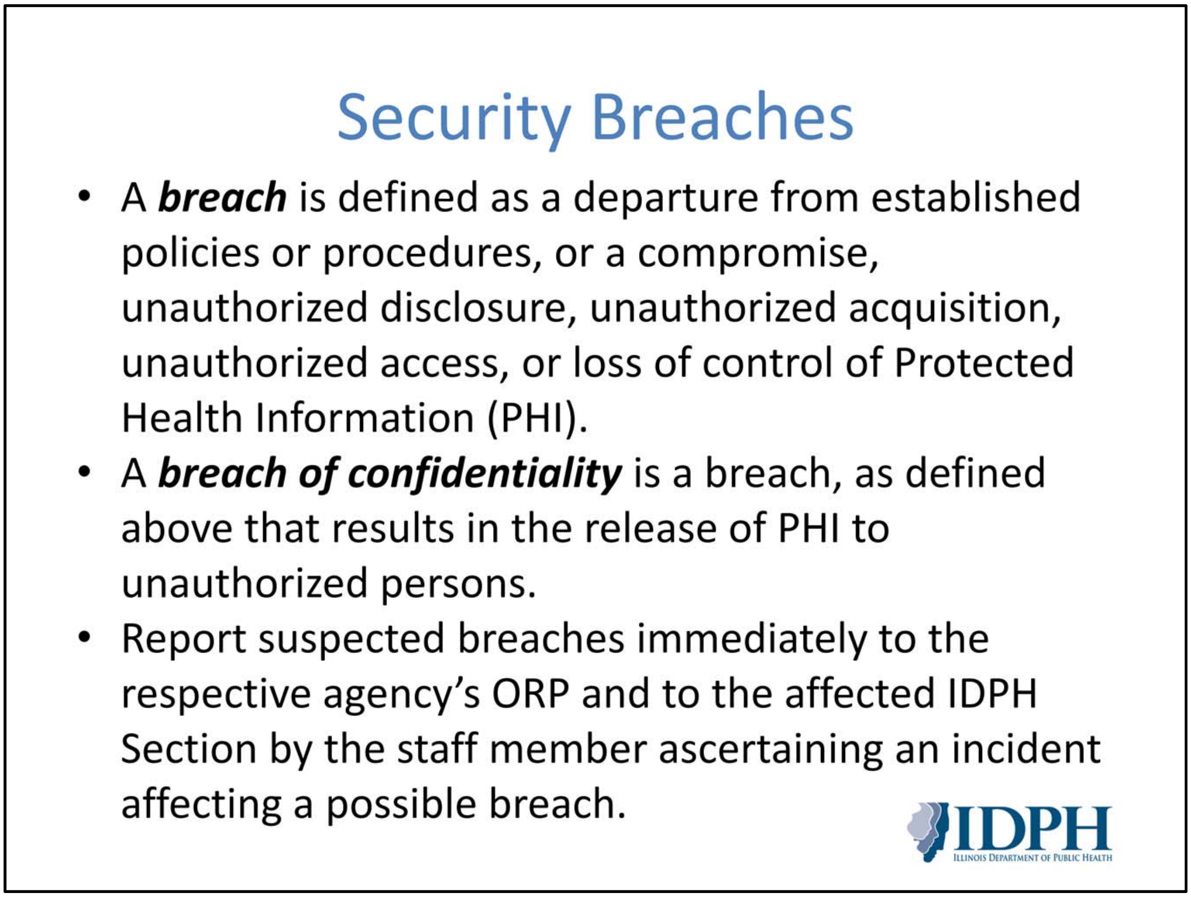
IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

In some situations, email may be your only contact information for a client. If this is the case:

- Email can be used as a last resort and no confidential information can be shared.
- The e-mail must not make any reference to any specific disease/infection (including in your e-mail signature, header, footer, or through clipart images).
- For agencies providing care to HIV positive clients only, or if an ***agency's email address includes the words HIV, AIDS or related terms***, a general email address void of these references should be created to minimize the likelihood of alerting a non-authorized person that the email is related to one's HIV status.
- Only leave your contact information in the e-mail.

Fax transmission of confidential or identifiable information should only be used as last resort, and faxes should be sent to a fax machine kept in a confidential, secure area.

In some cases, health department offices only have one fax, located in a communal area. If this is the case, and a fax must be sent, then the sender should call ahead before sending the fax in order to notify the recipient by phone and ensure that someone is available to receive the fax as soon as it prints out. This minimizes the possibility of someone else intercepting the confidential fax.



Security Breaches

- A ***breach*** is defined as a departure from established policies or procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of Protected Health Information (PHI).
- A ***breach of confidentiality*** is a breach, as defined above that results in the release of PHI to unauthorized persons.
- Report suspected breaches immediately to the respective agency's ORP and to the affected IDPH Section by the staff member ascertaining an incident affecting a possible breach.

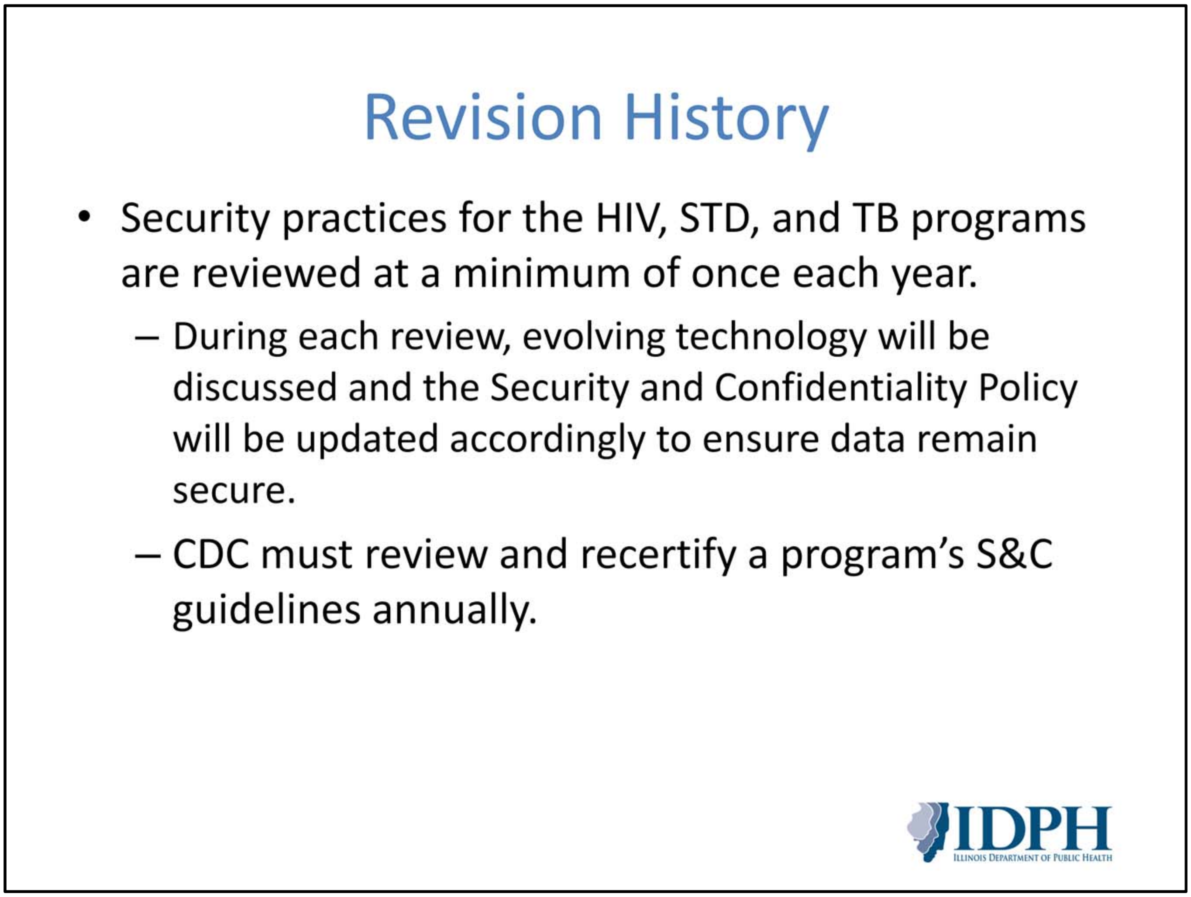
IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

A **breach** is defined by the CDC as a departure from established policies or procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of Protected Health Information (PHI). A breach is an infraction or violation of a policy, standard, obligation, or law. A breach in data security would include any unauthorized use of data, even aggregated data without names. A breach may be malicious or unintentional.

A **breach of confidentiality** is a breach, as defined above, that results in the release of PHI to unauthorized persons (such as other employees or members of the general public).

ALL suspected breaches of confidentiality should be reported immediately to IDPH anytime a breach is suspected, regardless of whether or not the breach results in the release of confidential information to an unauthorized person. Breaches of confidentiality can be reported to the Section Chief or program administrator at IDPH (such as the HIV Surveillance, Prevention or Direct Services administrators) by the staff member ascertaining an incident affecting a possible breach.

If confidential information is released, the breach will be reported to CDC. If confidential information is not released, the breach will be handled by the state health department and not reported to CDC. A log will be maintained to detect patterns of breaches and track compliance.



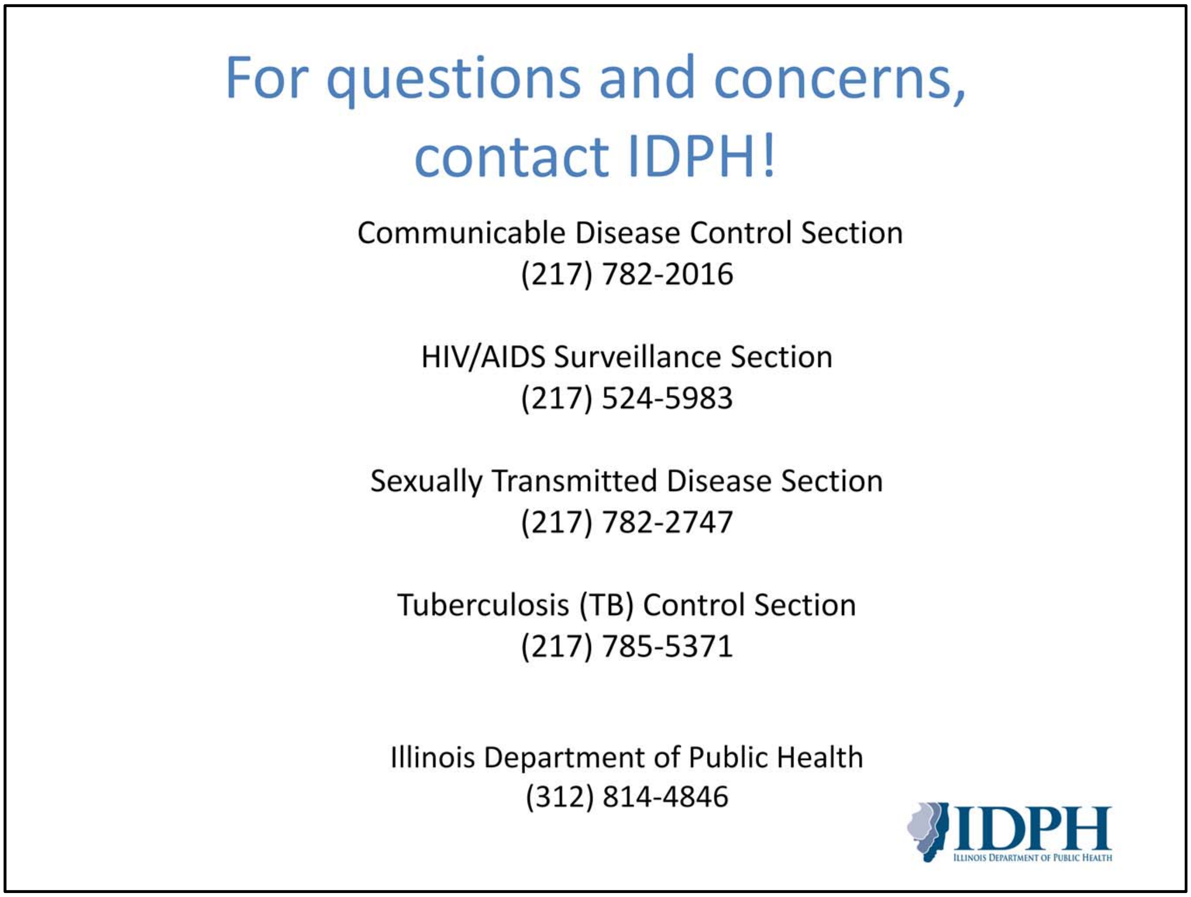
Revision History

- Security practices for the HIV, STD, and TB programs are reviewed at a minimum of once each year.
  - During each review, evolving technology will be discussed and the Security and Confidentiality Policy will be updated accordingly to ensure data remain secure.
  - CDC must review and recertify a program's S&C guidelines annually.

IDPH
ILLINOIS DEPARTMENT OF PUBLIC HEALTH

Security practices for the HIV, STD, and TB programs are reviewed each year. During each review, evolving technology will be discussed and the Security and Confidentiality policy will be updated accordingly to ensure data remain secure.

CDC will review and recertify the Security and Confidentiality guidelines each year in order for programs to be refunded for activities.



For questions and concerns, contact IDPH!

Communicable Disease Control Section
(217) 782-2016

HIV/AIDS Surveillance Section
(217) 524-5983

Sexually Transmitted Disease Section
(217) 782-2747

Tuberculosis (TB) Control Section
(217) 785-5371

Illinois Department of Public Health
(312) 814-4846

IDPH
Illinois Department of Public Health

For more information, or if you have concerns that a policy cannot be met, or for questions regarding specific policies, please feel free to contact the Illinois Department of Public Health Program Administrators