

Active Responsible Stewardship: From Training to Responding

CSTE webinar series

Implementing the Integrated Data Security and Confidentiality
Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease,
and Tuberculosis Programs

August 26, 2013

1:00 – 2:15 pm ET



COUNCIL OF STATE AND
TERRITORIAL EPIDEMIOLOGISTS

Webinar Agenda

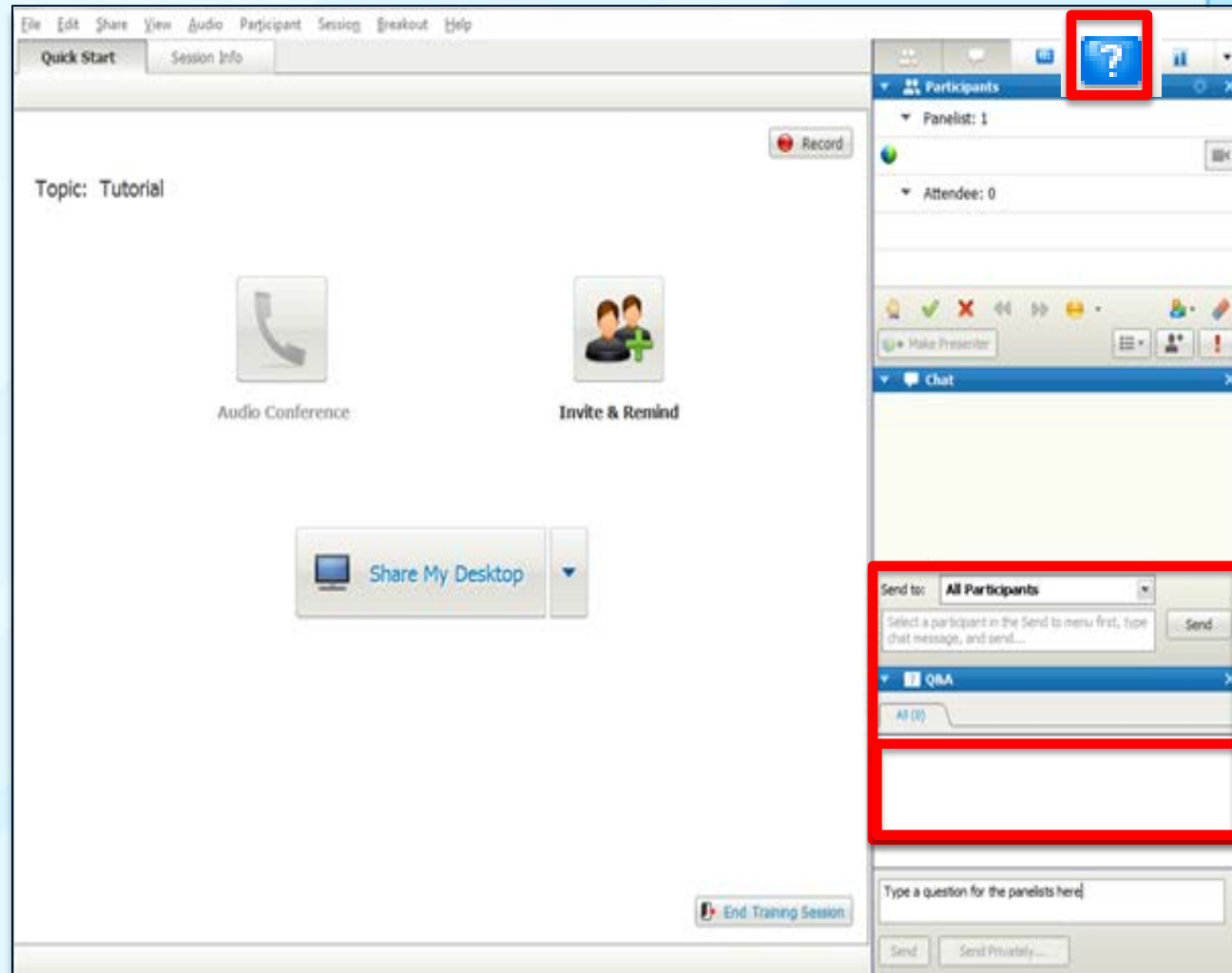
- **Moderator: Vincent Fears, Program Consultant/Project Officer, Division of TB Elimination**
- Introduction and Welcome: Gustavo Aquino, Associate Director for Program Integration, NCHHSTP
- Patricia Sweeney, Senior Epidemiologist, HIV Incidence and Case Surveillance Branch, DHAP, CDC
- Medina Tipton, HIV/AIDS Surveillance Coordinator, Kentucky Department for Public Health
- Lou Smith, Director of Division of Epidemiology, Evaluation and Research at the AIDS Institute, New York State Department of Health
- Questions and Discussion: presenters and participants

Webinar Housekeeping

- **Please note that today's webinar is being recorded**
 - The webinar recording, presentation slides, and additional tools and templates will be available in the webinar library on CSTE's website:
<http://www.cste.org/?page=WebinarLibrary>
- **All phone lines have been placed on mute**
- **There will be a question-and-answer session at the end of the webinar**
 - To ask a question, please use the Q&A box on the right side of your screen

To Ask a Question

- Click on the blue question mark tab on the top right panel of your screen
- This will open the Q&A box on the bottom right panel on your screen
- Type a question
- Send questions to All Panelists
- Questions will be answered during the Q&A period



Webinar Agenda

- Moderator: Vincent Fears, Program Consultant/Project Officer, Division of TB Elimination
- **Introduction and Welcome: Gustavo Aquino, Associate Director for Program Integration, NCHHSTP**
- Patricia Sweeney, Senior Epidemiologist, HIV Incidence and Case Surveillance Branch, DHAP, CDC
- Medina Tipton, HIV/AIDS Surveillance Coordinator, Kentucky Department for Public Health
- Lou Smith, Director of Division of Epidemiology, Evaluation and Research at the AIDS Institute, New York State Department of Health
- Questions and Discussion: presenters and participants

Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, STD, and TB

Active Responsible Stewardship: *From Training to Responding*

Introduction and Welcome

Gustavo Aquino

Associate Director for Program Integration

CDC/OID/NCHHSTP

August 26, 2013

Webinars will now be available...

Webinars recorded and available online in the Webinar library at www.cste.org

- ✓ The First Step: Conducting an Initial Assessment
- ✓ Developing Policies & Procedures and Periodic Assessments
- ✓ Creating a Confidential and Secure Physical & Electronic Environment and the Process of Certification and Validation
- ✓ Driving Public Health with Appropriate Data: Data Sharing – Why, When, Who and How?

Today's session

- ✓ Active Responsible Stewardship – From Training to Responding:

More Templates, Examples and Tools Coming

- ❑ **Templates and examples for implementing the 2011 NCHHSTP S&C Guidelines are being posted with the webinar recordings and slides at www.cste.org**
- ❑ **Look for these as they are posted at the time of each webinar and throughout the coming months**
- ❑ **Examples include**
 - Initial and Periodic Assessments Templates and Examples
 - Sample policies, procedures and forms

Webinar Agenda

- Moderator: Vincent Fears, Program Consultant/Project Officer, Division of TB Elimination
- Introduction and Welcome: Gustavo Aquino, Associate Director for Program Integration, NCHHSTP
- **Patricia Sweeney, Senior Epidemiologist, HIV Incidence and Case Surveillance Branch, DHAP, CDC**
- Medina Tipton, HIV/AIDS Surveillance Coordinator, Kentucky Department for Public Health
- Lou Smith, Director of Division of Epidemiology, Evaluation and Research at the AIDS Institute, New York State Department of Health
- Questions and Discussion: presenters and participants

Active Responsible Stewardship – From Training to Responding Overview

Patricia Sweeney

HIV Incidence and Case Surveillance Branch
Division of HIV/AIDS Prevention

Guiding Principle 10: Program officials should be active, responsible stewards of public health data.



What is Stewardship?

STEWARDSHIP (merriam-webster.com)

1: the office, duties, and obligations of a steward

2 : the conducting, supervising, or managing of something; *especially*: the careful and responsible management of something entrusted to one's care

What encompasses active, responsible stewardship of public health data?

- ❑ Policies and procedures
- ❑ Training
- ❑ Roles and responsibilities
- ❑ Responding
- ❑ Reviewing
- ❑ Revising



Standards (1)

1.0 Program Policies and Responsibilities

Standard 1.1 Develop written policies and procedures on data security, them annually; revise them as needed; and make them accessible...

Standard 1.2 Designate an Overall Responsible Party(ORP)

Standard 1.3 Ensure policies define the roles and access levels of all persons with authorized access

Standard 1.4 Ensure policies require ongoing reviews of evolving technologies and include a computer back-up or disaster recovery plan

* Note standards may be paraphrased for this presentation.

Standards (2)

1.0 Program Policies and Responsibilities

Standard 1.5 Ensure that any breach of data security protocol, regardless of whether personal information was released, is reported to the ORP and investigated immediately. Any breach that results in the release of PII to unauthorized persons should be reported to the ORP, to CDC, and, if warranted, to law enforcement agencies.

* Note standards may be paraphrased for this presentation.

Standards (3)

1.0 Program Policies and Responsibilities

Standard 1.6 Ensure that staff members with access to identifiable public health data attend data security and confidentiality training annually.

Standard 1.7 Require all newly hired staff members to sign a confidentiality agreement before given access to identifiable information; require all staff members to re-sign their confidentiality agreements annually.

* Note standards may be paraphrased for this presentation

Standards (4)

1.0 Program Policies and Responsibilities

Standard 1.8 Ensure that all persons who have authorized access to confidential public health data take responsibility for

- 1) implementing the program's data security policies and procedures,
- 2) protecting the security of any device in their possession on which PII are stored, and
- 3) reporting suspected security breaches.

Guiding Questions

- ☐ Are procedures in place to respond to breaches in data security?
- ☐ Do you have a checklist of steps to follow in case of a breach?
- ☐ Does the data security policy identify the person(s) to be notified if a breach is suspected?
- ☐ Are staff members familiar with the program's definition of a security breach?
- ☐ Do you record or log all breaches and responses?
- ☐ Is there a process to review lessons learned?

Responding to Breaches

Definitions

Confidentiality Breach - Situation in which persons other than authorized users, or for other than authorized purpose, have access to PII

Policy or Protocol Violation - Incidents where policies are breached but only authorized individuals have had access

Reporting of Policy Violations and Breaches in Confidentiality

- ☐ Policy violations that did not involve release of PII can be handled within programs with notification of the ORP(s)
 - ☐ Note: additional state reporting requirements may apply
- ☐ When in doubt report and ask
- ☐ Breaches involving disclosure of PII involving federal data or federally supported systems should be reported to ORP, supervisor, and CDC
- ☐ OMB requires notification to funding agency (HHS) within 60 minutes of discovery of breaches of PII from federally supported data systems
- ☐ OMB Memorandum 06-19
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf>

Reporting of Policy Violations and Breaches in Confidentiality to CDC

Who do I notify at CDC?

- Notify applicable CDC program project officer or designated official and
- Ralph Vaughn, NCHHSTP Information Systems Security Officer (ISSO) Phone: 404.429.8710 email: RVaughn@cdc.gov

What information will I be asked for?

- What happened, where, and when?
- What data collection system was involved?
- What PII and other information, including clinical status was involved?
- Were electronic systems breached or hard copy records involved?
- How many records or people were involved?
- What entity (HD, CBO, etc.) was involved and how were they funded for this data collection (COAG, Contract, Subcontract)?

Additional follow-up may be required

Training

- **Annual**
- **In person or web based**
- **Scenarios and other tools may be useful**
- **Review of SOPs**
- **Specific to role and access to PII**
- **Opportunity to sign confidentiality agreement**

Training

Annual training should include:

- ☐ **Review of personal responsibilities**
- ☐ **Procedures for ensuring physical security of PII**
- ☐ **Procedures for electronically storing and transferring data**
- ☐ **Policies and procedures for data sharing**
- ☐ **Procedures for reporting and responding to security breaches**
- ☐ **Review of relevant laws and regulations**

Contact Information

- ❑ *Resources (including links to CSTE site) available on the PCSI website:*
<http://www.cdc.gov/nchhstp/programintegration/>
- ❑ Send questions to pcsi@cdc.gov
- ❑ Patricia Sweeney
psweeney@cdc.gov

Webinar Agenda

- Moderator: Vincent Fears, Program Consultant/Project Officer, Division of TB Elimination
- Introduction and Welcome: Gustavo Aquino, Associate Director for Program Integration, NCHHSTP
- Patricia Sweeney, Senior Epidemiologist, HIV Incidence and Case Surveillance Branch, DHAP, CDC
- **Medina Tipton, HIV/AIDS Surveillance Coordinator, Kentucky Department for Public Health**
- Lou Smith, Director of Division of Epidemiology, Evaluation and Research at the AIDS Institute, New York State Department of Health
- Questions and Discussion: presenters and participants

Web-based Security and Confidentiality Training: Kentucky's Approach

Medina Tipton

HIV Surveillance Coordinator

Kentucky Department for Public Health

An idea was conceived

- ❑ **Annual training is a requirement with in S & C requirements.**
- ❑ **New staff (particularly outside of HIV surveillance) change constantly with little notice**
- ❑ **How can you gather all the departments involved to come to ONE training?**
 - **By attempting online training.**

Multiple paths to same destination

- ❑ **Can do both-in person or virtual**
 - Annual training
 - New hire training
- ❑ **Sometimes help with questions and situations that are being seen in the field**
- ❑ **Just one way to conduct training**

A TRAIN is coming

- ❑ **TRAIN is an online based program.**
 - Manned by a staff of 5 persons
 - Responsible for the cyber upkeep of the modules
 - Content is strictly the author's responsibility
 - Format is similar to a very complicated power point presentation.

TRAIN

- ❑ Was the idea of a public health student at the University of Kentucky.
- ❑ Several other similar modules on the market
- ❑ Kentucky selected TRAIN due to
 - cost
 - flexibility of format
 - emphasis on public health.

How it was done

- ❑ **First looked at the security and confidentiality policy and pulled out all the information that needed to be covered.**
- ❑ **Decided format of module**
 - Information (with embedded documents)
 - Post Test
 - Evaluation
- ❑ **Decided how to best group the information**
 - Clear
 - Concise
 - Not sleep inducing

To Ensure Compliance

- ❑ Stated that failure to take this course will prevent access to HIV/AIDS information.**
- ❑ Included the S&C policy and the non-disclosure agreement within the module to be signed**
- ❑ Had test at the end that participants had to pass to receive certificate.**

SCORM Player - Windows Internet Explorer

http://training.chfs.ky.gov/asp_net/scorm/prodplayer/Index.htm?uc=338481&randomNumber= Bing

File Edit View Favorites Tools Help

★ Favorites Outreach.NET Login Suggested Sites Web Slice Gallery

SCORM Player

Quit

PHF
Public Health Foundation

Security and Confidentiality Training for HIV/AIDS surveillance

HOME HELP EXIT BACK NEXT

Welcome!

To navigate throughout this course, please click the Back and Next buttons located at the lower right corner.

The Help, Home, and Exit buttons are located at the top right, for your convenience.

There is a Drop-Down navigation bar which includes a Table of Contents that will take you to specific chapters and pages within the module.

You can also click the Help button to e-mail the Course Administrator, [Medina Tipton](#)

This module will take approximately 20 minutes to complete.

If this module does not display properly, you may have to download

Done Local intranet 100%

Start » Inbox - ... HIV/AIDS... Abstract... Microsoft... KMI's eLM... SCORM ... 5:17 PM

Quit



HIV/AIDS Branch Surveillance Security Policy

Please click the document image below to view a PDF version of the complete HIV/AIDS Branch Surveillance Security Policy.



SCORM Player - Windows Internet Explorer

http://training.chfs.ky.gov/asp_net/scorm/prodplayer/Index.htm?uc=338481&randomNumber=

File Edit View Favorites Tools Help

★ Favorites ★ Outreach.NET Login Suggested Sites Web Slice Gallery

SCORM Player


Quit

PHF
Public Health Foundation

HOME HELP EXIT BACK NEXT

Physical Security Continued

- Sit behind double locked doors, windows are locked and covered with blinds
- All paperwork, flash drive, etc is locked in a fire-proof and bomb-proof cabinet with double locks
- If on site visit, all paperwork must remain in surveillance staff possession and is locked in a briefcase that is in the locked trunk of a locked car
- Surveillance personnel cannot confirm or deny if cases are previously reported to health practitioners, infection control nurses, etc.



Local intranet 100%

Start Inbox - ... HIV/AIDS Abstract... Microsoft... KMi's eL... SCORM ... 5:27 PM

SCORM Player - Windows Internet Explorer

http://training.chfs.ky.gov/asp_net/scorm/prodplayer/Index.htm?uc=338481&randomNumber= Bing

File Edit View Favorites Tools Help

Favorites Outreach.NET Login Suggested Sites Web Slice Gallery

SCORM Player

Quit

PHF
Public Health Foundation


HOME HELP EXIT BACK NEXT

Electronic Security

eHARS server is located in Commonwealth data center. Connectivity is protected by firewall rules and server access is locked down. All computers with eHARS must be logged off/turned off at the end of the day and require password to log in.
Satellite office staff connects by secure VPN connection.

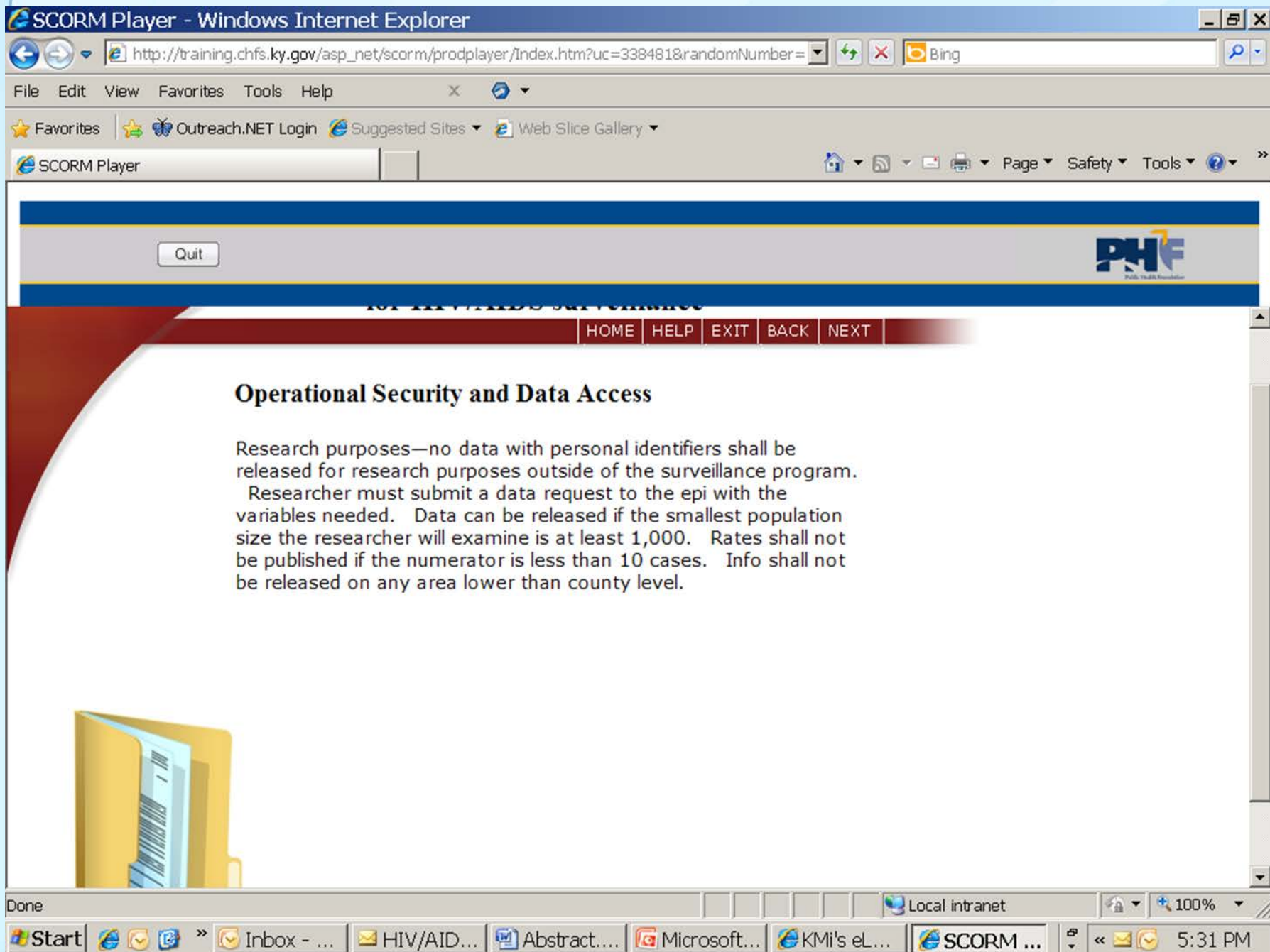
Diskettes, USB flash drives with personal identifiers must include only minimal amount of information necessary to perform tasks. It will be encrypted and stored under lock and key when not used.

IT authorities must obtain approval from the surveillance coordinator before adding users to any HIV/AIDS surveillance program application. IT shall maintain logs documenting authorized users. The surveillance coordinator shall review logs annually.



Done Local intranet 100%

Start Inbox - ... HIV/AID... Abstract... Microsoft... KMI's eL... SCORM ... 5:29 PM



Quit

[HOME](#) [HELP](#) [EXIT](#) [BACK](#) [NEXT](#)

Operational Security and Data Access

Research purposes—no data with personal identifiers shall be released for research purposes outside of the surveillance program.

Researcher must submit a data request to the epi with the variables needed. Data can be released if the smallest population size the researcher will examine is at least 1,000. Rates shall not be published if the numerator is less than 10 cases. Info shall not be released on any area lower than county level.

Post Test

SCORM Player - Windows Internet Explorer

http://training.chfs.ky.gov/asp_net/scorm/prodplayer/Index.htm?uc=687008&randomNumber=B0D891BC-2D16-42FC-B283-7F7C3E

File Edit View Favorites Tools Help

★ Favorites SCORM Player

Convert Select Page Safety

Security and Confidentiality Training for HIV/AIDS surveillance

HOME HELP EXIT BACK NEXT

1. All DPH staff can open confidential HIV/AIDS surveillance mail.

☒ True

☐ False

Back Cancel Next

Page 25 of 31

Local intranet | Protected Mode: Off 125%

Post Test

SCORM Player - Windows Internet Explorer

http://training.chfs.ky.gov/asp_net/scorm/prodplayer/Index.htm?uc=687008&randomNumber=B0D891BC-2D16-42FC-B283-7F7C3E

File Edit View Favorites Tools Help

SCORM Player

Convert Select

Page Safety

Security and Confidentiality Training for HIV/AIDS surveillance

HOME HELP EXIT BACK NEXT

4. Who are the two state public health agencies that are allowed to receive personal information when released to designated persons:

- ☐ a. STD and Viral Hepatitis
- ☐ b. TB and Reportable Disease
- ☐ c. TB and STD
- ☐ d. None of the above

Back Cancel Next

Page 28 of 31

Local intranet | Protected Mode: Off 125%

Evaluation

Evaluation - Windows Internet Explorer

https://ky.train.org/DesktopModules/eLearning/Evaluations/CourseEvaluation.aspx?co

File Edit View Favorites Tools Help

Favorites Outreach.NET Login Suggested Sites Web Slice Gallery

Evaluation

HIV/AIDS Security and Confidentiality Training Mod - Question 1 of 12.

Rate how well this course objective was met: To understand the physical and electronic security measures to safeguard the confidentiality of information collected by the HIV/AIDS surveillance office.

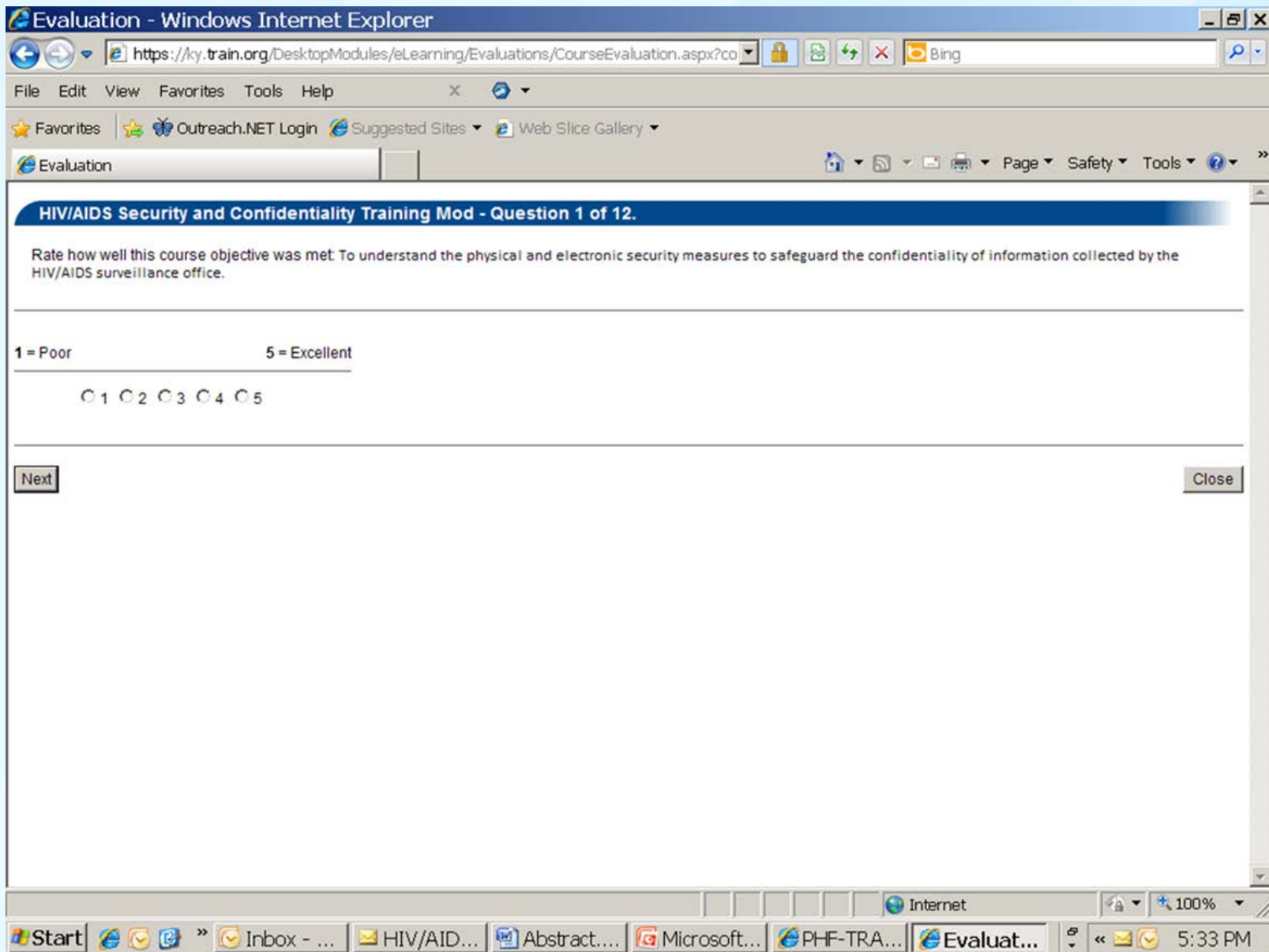
1 = Poor 5 = Excellent

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Next Close

Start Internet 100% 5:33 PM

Inbox - ... HIV/AIDS... Abstract... Microsoft... PHF-TRA... Evaluat...





Next Steps

- ❑ To continue to add real-life situations and how they should be solved.
- ❑ More in-depth feedback
- ❑ Major update with the new S&C guidelines

Did it work

- ❑ For Kentucky—YES
- ❑ Examine the staff and structure of your surveillance program

In conclusion

- ❑ Online training is helpful to meet the annual training requirement of Security and Confidentiality.
- ❑ See if your state has TRAIN or an equivalent.
- ❑ This is only a guide.....

Contact information

Medina Tipton

HIV/AIDS Surveillance Coordinator

Kentucky Department for Public Health

Medina.Tipton@ky.gov

502-564-6539x4287

Webinar Agenda

- Moderator: Vincent Fears, Program Consultant/Project Officer, Division of TB Elimination
- Introduction and Welcome: Gustavo Aquino, Associate Director for Program Integration, NCHHSTP
- Patricia Sweeney, Senior Epidemiologist, HIV Incidence and Case Surveillance Branch, DHAP, CDC
- Medina Tipton, HIV/AIDS Surveillance Coordinator, Kentucky Department for Public Health
- **Lou Smith, Director of Division of Epidemiology, Evaluation and Research at the AIDS Institute, New York State Department of Health**
- Questions and Discussion: presenters and participants

MAINTAINING A CULTURE OF STEWARDSHIP: PREVENTING AND MANAGING BREACHES

Lou Smith, MD, MPH

**Division of Epidemiology, Evaluation and Research
AIDS Institute**

New York State Department of Health

August 26, 2013

Legal and Organizational Environment for HIV Surveillance in New York State

Timeframe	Legal	Organizational
1980's	Article 27F established penalties for sharing HIV/AIDS data with unauthorized persons	HIV/AIDS surveillance within Division of Epidemiology (separate from AIDS Institute)
2000	NYS HIV Reporting and Partner Notification Law established name-based HIV reporting and use of surveillance data for epidemiology and HIV partner services only	HIV Partner Services developed within Bureau of STD Control as joint STD/HIV program with state staff in 5 regional offices & county staff in 12 counties; New York City programs
2010	HIV Testing Law broadened use of surveillance data to include assessment of co-morbidity, completeness of reporting, and meeting programmatic needs	Realignment of HIV surveillance and STD control within the AIDS Institute which is responsible for HIV and hepatitis programmatic activity

Approach to Data Security and Confidentiality

- Program policies and responsibilities
 - Individual roles and responsibilities
 - Annual training; confidentiality agreements
 - Designation of overall responsible party (ORP)
- Data collection and use
- Secure environment for data
 - Physical security
 - Electronic security
- Data sharing and release
- Management of policy violations and breaches of confidentiality
- Program policies reviewed routinely and in response to policy violations and breaches; policies updated

Roles and Responsibilities

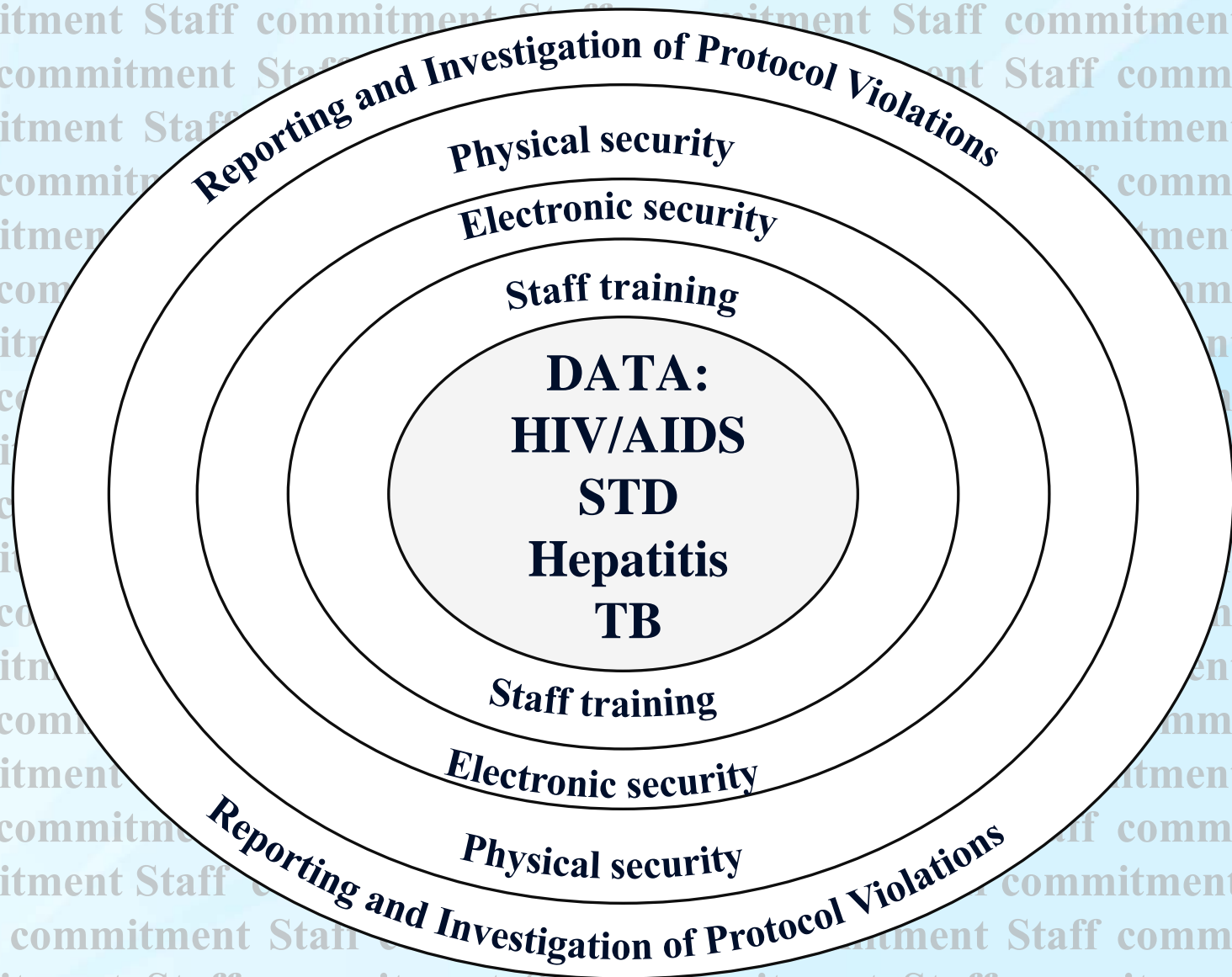
- Security of surveillance information is the joint responsibility of many participants in the New York State public health system
 - Individual employees
 - Coworkers
 - County and regional supervisory staff
 - NYSDOH bureaus, divisions, and centers
 - LORP and ORP (Overall Responsible Party)

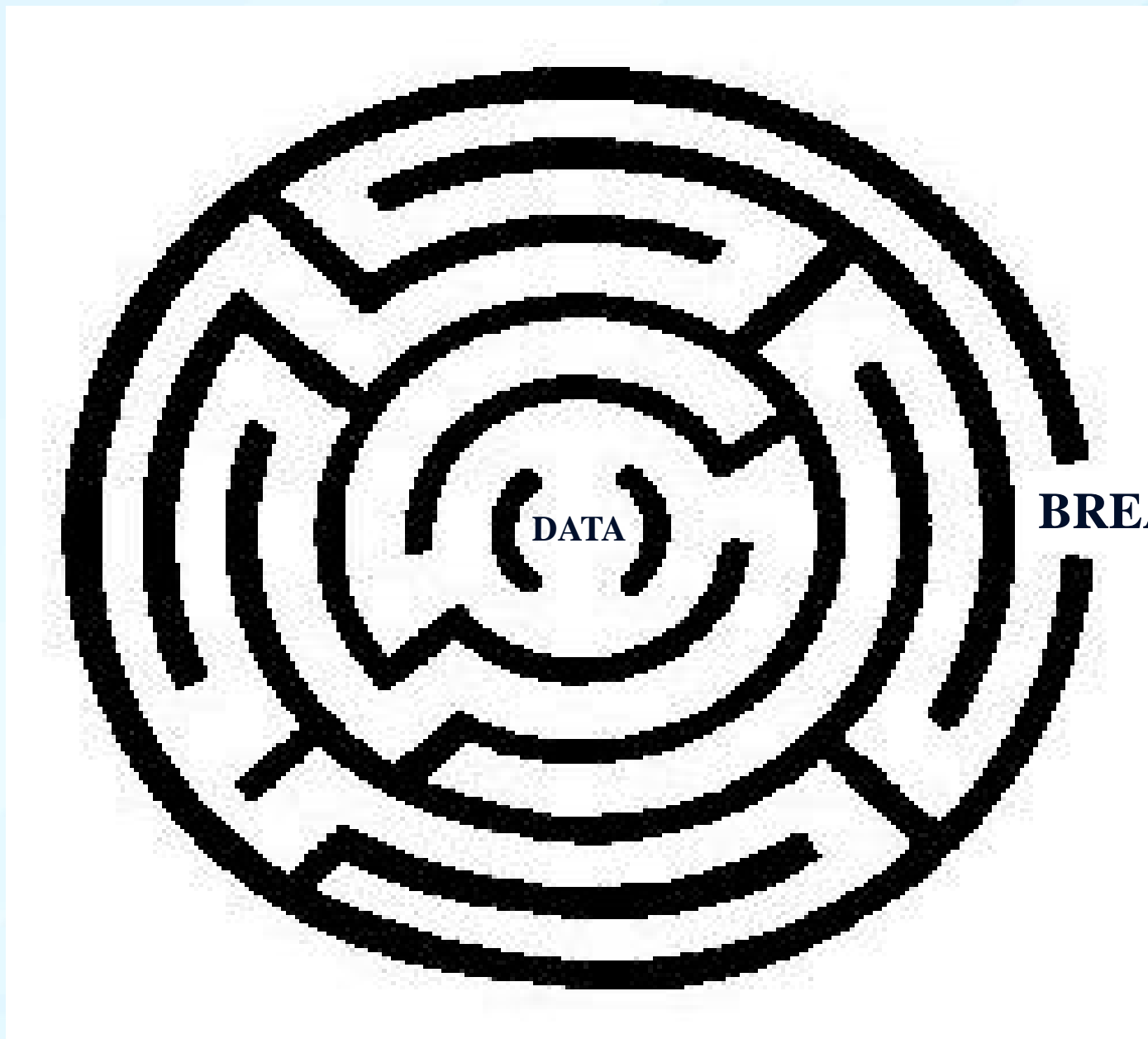
Individual Responsibility: Do You Know...?

- Where can you access a copy of your unit's confidentiality policies?
- Who is the LORP or ORP for your office?
- How should arrangements be made for new employee training?
- No manual or training can cover everything. If in doubt, who do you ask for guidance?

Security: Policy or Protocol Violation vs. Breach of Confidentiality

- **Policy or Protocol Violation**
 - Incidents where policies are breached—e.g., actions are contrary to existing policies
- **Breach of Confidentiality**
 - Situation in which persons other than authorized users have access to confidential information, or authorized users access confidential information for a non-authorized purpose





Prevention - 1

- Confidentiality training for all new employees
- Annual training updates with confidentiality agreement (attestation)
 - Employee is stating that s/he understands and agrees to abide by policies
 - Proof of signed attestation required before release of passwords and keys
- Written policies and procedures, including physical and electronic security measures, implemented and available for reference
- A culture of respect for confidentiality and mutual assistance in adhering to policies
 - From the NYSDOH HIV Surveillance Policies and Procedures: “Each employee ...must diligently report all suspected and actual breaks in protocol and breaches of confidentiality immediately to the designated supervisor. Failure to report is itself a violation.”

Prevention - 2

- Investigate questions or problems promptly and document actions
 - Close the loop on existing questions
 - Have local procedures for documentation
- Anticipate new areas of vulnerability. Typically, a time of change is a time of vulnerability
 - Changing technology
 - New equipment or software
 - New staff or new staff responsibility
 - Change in location
 - Unusual but legitimate need for broader communication of information

Prevention – 3

- Discuss ideas/needs for policy updates with local supervisory staff and/or staff responsible for confidentiality and security policies
- Tool (questionnaire) used for annual monitoring of site compliance with existing policies
 - completed by regional or county supervisor acting on behalf of the Local Overall Responsible Party (LORP)

Prevention – 4

- New York Times Editorial September 25, 2006:

*“In the early days of the AIDS epidemic, the disease carried such a stigma that people shied away from being tested lest they be socially ostracized or suffer discrimination. Patient advocacy groups pushed hard for policies to limit how testing was done and make sure all patients were counseled on the ramifications, both good and bad, before consenting to let their blood be tested. But times have changed. New treatments make it valuable to learn whether someone is infected. **Health officials have shown that they can be trusted to keep test results confidential.**”*

- Press reports

- Emerging issue in data security and confidentiality
- Third-party perspective

Assessing a Data Security Problem: First Steps

- Rescue! Is highly confidential data at ongoing risk? What can be done to minimize or eliminate the ongoing risk?
- Does the problem constitute a protocol violation or a breach in confidentiality?
- If the problem is not a breach in confidentiality or technically even a protocol violation, what led to the question?
 - A bad idea or poor judgment
 - “Can’t see the forest for the trees”
 - Thoughtful assessment of a problem area

Handling Serious Protocol Violations

- Carry out previously delineated internal notifications
 - Supervisory structure, ORP
 - CDC if breach of confidentiality possible
- Investigate immediately to assess causes and implement remedies
 - Meet with involved employees and their supervisors
 - Counsel recipient of information if appropriate
 - Analyze errors of commission/omission
- Develop and implement a plan for correction
 - Appropriate corrective action may include disciplinary action
 - Document finding/actions in security log
 - NYSDOH policy is written report
 - Description of incident
 - Steps taken to ensure that the protocol violation is not repeated in the future

Managing Possible or Definite Breaches of Confidentiality

- Conduct same activities as with break in protocol
 - Immediately notify previously delineated senior staff, including LORP, ORP and CDC
 - Meet with involved employees and their supervisors
 - Counsel recipient of information if appropriate
 - Analyze errors of commission/omission
 - Develop and implement a plan for correction
 - Take appropriate corrective action which may include instituting disciplinary actions
 - Document finding/actions in security log
- Timely final written report

Managing Breaches of Confidentiality - 1

- NYSDOH ORP will convene a committee
 - ORP
 - Supervisory staff of employee(s) associated with breach
 - Senior epidemiology staff
 - DOH Legal Affairs
 - As warranted, include or consult with
 - Representatives of other agencies involved in breach
 - Privacy officer, HIPAA officer
 - Press officer
 - Senior IT officials
 - Human resources

Managing Breaches of Confidentiality - 2

- Committee deliberations
 - Extent or scope of disclosure
 - Severity of damage
 - Intentional or non-intentional nature of disclosure
 - Episodic or systemic nature of breach
 - Previous conduct or infractions involving the same employee or unit
 - Legal implications
 - Need for notification of persons whose confidentiality was breached
 - Action plan

Other Considerations in Evaluating Breaches

- Was the employee's personal well-being threatened?
- Did an illegal act occur?
- Was the employee appropriately trained and supervised?
Do the employee's supervisor/coworkers share culpability?
- Was the action willful? Does the employee have a track record of carelessness or disregard for confidentiality?

Maintaining a Culture of Stewardship: Ongoing NYSDOH Efforts

- Aligning approaches to HIV, STD, TB, and hepatitis surveillance data and HIV programmatic data
 - HIV and STD surveillance have a long history of similar policies
 - Common Overall Responsible Party
 - Different legal authority
 - Varying locations and organizational and administrative structures
- Maintaining updated policies and procedures, particularly with technological advances and institutional technological changes
- Principles of prevention and management of breaches remain the same

Contact Information:

Lou Smith, MD, MPH

**New York State Department of Health
Division of Epidemiology, Evaluation and Research
AIDS Institute
Albany, NY 12237**

lls04@health.state.ny.us

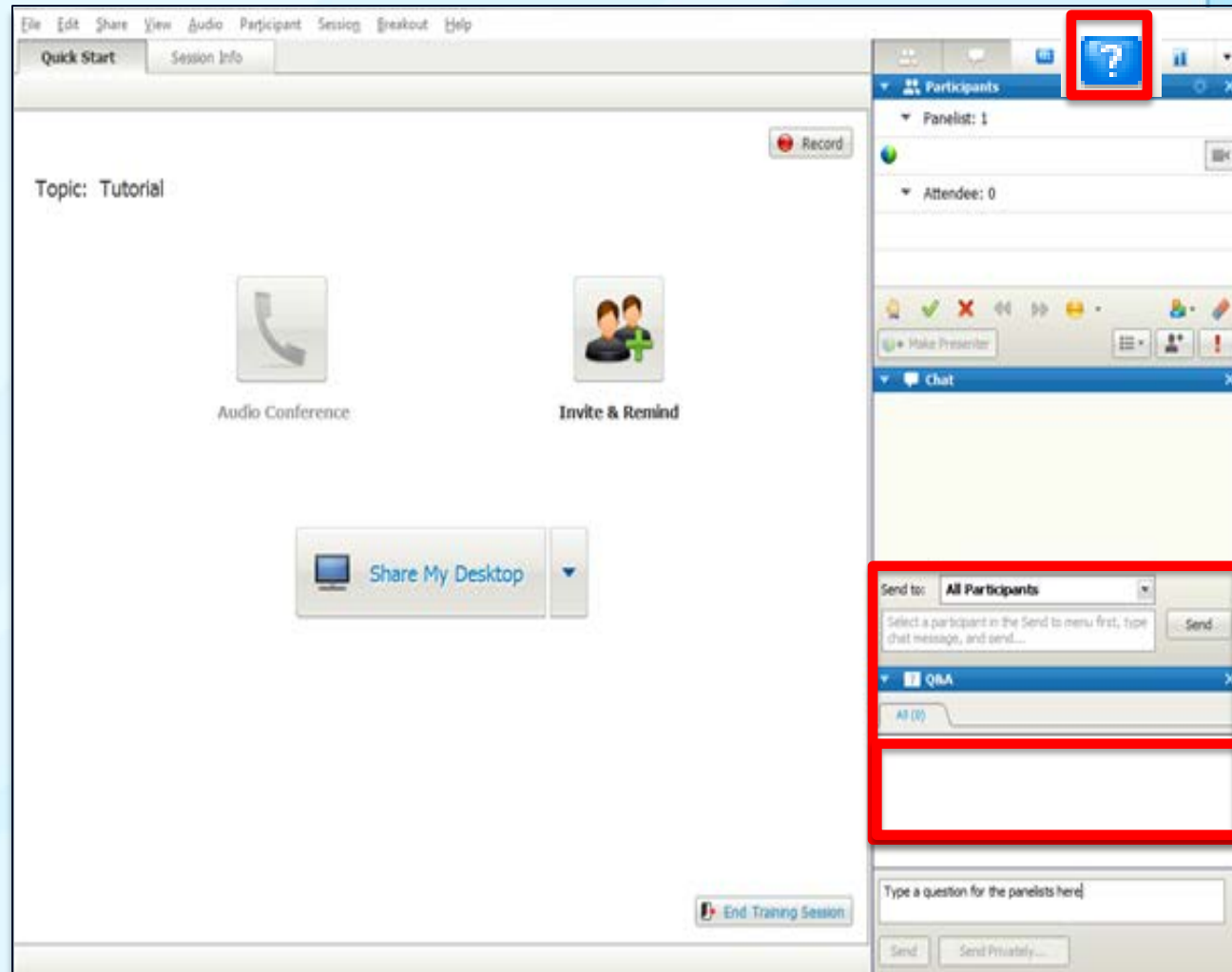
Phone: (518) 474-7238

Webinar Agenda

- Moderator: Vincent Fears, Program Consultant/Project Officer, Division of TB Elimination
- Introduction and Welcome: Gustavo Aquino, Associate Director for Program Integration, NCHHSTP
- Patricia Sweeney, Senior Epidemiologist, HIV Incidence and Case Surveillance Branch, DHAP, CDC
- Medina Tipton, HIV/AIDS Surveillance Coordinator, Kentucky Department for Public Health
- Lou Smith, Director of Division of Epidemiology, Evaluation and Research at the AIDS Institute, New York State Department of Health
- **Questions and Discussion: presenters and participants**

To Ask a Question

- Click on the blue question mark tab on the top right panel of your screen
- This will open the Q&A box on the bottom right panel on your screen
- Type a question
- Send questions to All Panelists



Thank you for your participation!

- Please complete today's webinar evaluation by Friday, Sept. 6:
<https://www.research.net/s/SCwebinar5>
- Please complete the overall webinar series evaluation by Friday, Sept. 13:
https://www.surveymonkey.com/s/cste_dataSCoverall
- The webinar recording & slides will be available CSTE's website in the webinar library: <http://www.cste.org/?page=WebinarLibrary>