Protecting the Public's Health while Ensuring Data Security and Confidentiality

Objective and Audience

This training provides an overview of the security and confidentiality policies and practices required of staff working with confidential information (CI) held by the MDPH Bureau of Infectious Disease and Laboratory Sciences (BIDLS).

This training is meant for all BIDLS staff, IT support staff, volunteers, interns, and contractors who have access to confidential information held by BIDLS.

Purpose

Our work within BIDLS permits access to extremely sensitive health information.

As stewards of these data, we have the responsibility to maintain the public's trust.

Failure to do so will impair our ability to protect the public from infectious disease.

Staff and Volunteer Responsibilities

- Complete MDPH and BIDLS confidentiality and data security trainings at hire and annually
- Follow policies, and associated protocols and procedures
- Ensure CI is protected
- Never share your password(s)
- Access information on a need-to-know basis

Staff Responsibilities (con't)

- Report any confidentiality or privacy breaches to Division Director and Overall Responsible Party (ORP)
- Before accessing CI, you must
  - Successfully complete this training
  - "Sign" (by clicking that you "agree") the confidentiality agreement at the end of this training
- Unauthorized access to confidential information is a serious concern and suspected incidents will be investigated immediately. Confirmed violations of confidentiality and data privacy will lead to corrective action

Overall Responsible Party (ORP)

- Overall Responsible Party (ORP): Catherine Brown, DVM, MSc, MPH, State Epidemiologist and State Public Health Veterinarian
  - The ORP has the responsibility for the security of the surveillance system (including processes, data, information, software, and hardware) and may have the liability for any breach of confidentiality.
  - This official has the authority to make decisions about surveillance operations.
  - The ORP is responsible for determining how surveillance information will be protected when it is collected, stored, analyzed, released, and dispositioned.

Laws, Regulations, and Standards

Laws, Regulations, and Standards

- MDPH is authorized to conduct activities related to the prevention and control of infectious diseases pursuant to its authority under M.G.L. c. 111, §§ 5, 6 & 7 and c. 111D, §6
  - Laws are implemented by 105 CMR 300.000: *Reportable Diseases, Surveillance and Isolation and Quarantine Requirements*
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
  - specifically allows public health reporting and access to protected health information (CI) for public health activities without requiring an individual's authorization (45 CFR 164.512)

Laws, Regulations, and Standards (con't)

- Federal assurance of confidentiality under section 308(d) of the Public Health Service Act
- CDC 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
- Recommendations of the National Institute of Standards and Technology (NIST)
- Massachusetts Fair Information Practices Act (FIPA)

Laws, Regulations, and Standards: STD and HIV

- Records of surveillance of sexually transmitted diseases are confidential pursuant to M.G.L. c. 111, §119, and may not be disclosed other than according to court order or where the Commissioner deems the information necessary to a person's public health duties.
- MDPH regulations 105 CMR 300.120(B) prohibit the disclosure of the identity of an individual with HIV or AIDS reported to the Department, including disclosure to any other local, state, or federal agency.

Laws, Regulations, and Standards: STD and HIV (con't)

- Records of HIV testing are confidential pursuant to M.G.L. c. 111, §70F, and may not be disclosed without the test subject's written consent
  - violation of §70F is deemed to be a violation of consumer protection law M.G.L. c. 93A §2

Maintaining Security and Confidentiality is Required by Regulation!

300.120: Confidentiality : All confidential personally identifying information, whether kept in electronic system or paper format, including but not limited to, reports of disease, records of interviews, written or electronic reports statements, notes, and memoranda, about any individual that is reported to or collected by the Department or local boards of health pursuant to 105 CMR 300.000 *et seq.*, shall be protected by persons with knowledge of this information. Except when necessary for the Commonwealth's or local jurisdiction's disease investigation, control, treatment and prevention purposes, or for studies and research authorized by the commissioner pursuant to M.G.L. c. 111, s. 24A, the Department and local boards of health shall not disclose any personally identifying information without the individual's written consent. Only those Department and local board of health employees who have a specific need to review personal data records for lawful purposes of the Department or local board of health shall be entitled access to such records. The Department and local boards of health shall ensure that all paper records and electronic data systems relating to information that is reported to or collected by the Department or local boards of health pursuant to 105 CMR 300.000 *et seq.,* are kept secure and, to the greatest extent practical, kept in controlled access areas.

Accessing Confidential Information (CI)

Bureau of Infectious Disease and
Laboratory Sciences

Access to CI

- Individuals are granted access to CI based on programmatic requirements and job responsibilities
- Access is limited on a need-to-know basis
- Individuals are not authorized to access CI outside of business hours without prior approval
- Individuals are not authorized to access CI offsite without prior approval
- Individuals are not authorized to search for information on individuals not directly related to case investigation/follow-up activities

Accessing CI in the Field

- Confidential information must not be accessed outside of work except for approved work-related purposes
  - ensure physical location is as secure as possible
- Written and dated approval must be given for staff who are typically not authorized to take documents home. CI must:
  - be transported in a secure container
  - not be visible in a car
  - contain the minimum amount of confidential information necessary to do business
  - where possible be coded to disguise any information that could easily be associated with disease and/or identify of the individual

Working with CI

- CI data must never be stored on personal devices
- CI must never be stored on a hard drive of any computer or laptop
- CI must not be downloaded to thumb drives or CD-ROMs, emailed or texted, unless you have specific approval
- Approved downloads of CI must be stored in secure folders and password protected
  - folders must be accessed by the minimally necessary number of individuals with a need to know
  - minimize the number of datasets in use and routinely delete after term of use has ceased

Working with CI (con't)

- Surveillance and epidemiological data must have personal identifiers removed when taken from a secure area and accessed from a non-secure area

Paper Formats

- When not in use, all documents with CI must be stored in a locked secure area
- Documents with CI must be returned to their secured storage after their use has been completed
- CI must not be readily observable by non-authorized users as they pass through the office, sit at desks, or approach reception areas

Electronic Formats

- E-mail and text transmissions are not considered secure, regardless of whether encrypted or if “secure:” is indicated in the subject line. Do not send CI via text or email unless with specific approval granted by the Privacy Office.
  - NB: the MAVEN ID and eHARS state number are to be considered as identifying variables when accompanied by additional case-based information

Electronic Formats (con't)

- If you receive CI through a non-secure method:
  - contact sender and indicate inappropriate use of email; request that the sender refrain from sending CI via email;
  - if responding via email, send a new email
  - delete all communications with CI from both email inbox and deleted items folders

Telephone

- Calls discussing CI must be made in a secure area
- Personnel must be reasonably certain that phone contacts are legitimate before discussing CI on the phone
- Share the minimum amount of CI to accomplish the surveillance or epidemiological objective of the call
- CI must never be left on voicemail systems unless they are secure systems or there is authorization from the call recipient to leave CI
  - **Do not identify yourself as being employed by ISIS or BIDLS, just the Department of Public Health**
- For outgoing voicemail messages, ask the caller to leave only their name and number and no CI

Fax and Scanners

- Fax machines and scanners used to send or receive CI must be located in a secure area
  - CI sent using fax must be faxed under a cover sheet
    - prior to sending, ensure recipient is available to receive fax
    - confirm that the information faxed was received by the intended recipient
- Scanned files that contain CI must be stored on a secure network drive or an encrypted device
  - images may be uploaded to specific events within MAVEN
- Do not send scanned files with CI (even encrypted) using email

Physical Security

Buildings and Offices

- all CI must be maintained in a secured locked area with limited access
- approved personnel will have access to confidential areas
- visitors to secured areas must be escorted at all times
- keys, key cards, and codes enabling access to secure areas must not be shared or loaned

Computer Workstations and Laptops

- computer screens must not be readily observable by non-authorized users as they pass through the office area, sit at desks, or approach reception areas

Data Release

- All data requests must be processed through ISIS, which will be triaged and responded in accordance with existing protocols
- Request for an individual's case information must be referred to ISIS. You may neither confirm nor deny that BIDLS holds information without authorized release
- With the exception of HIV/AIDS surveillance data, ISIS oversees data submissions to CDC; in general, data are sent to the CDC or any other agency subject to agreement and in accordance with approved methods

Document Disposal

- CI and other documents are maintained and destroyed according to the records retention policy for infectious disease surveillance and epidemiological information. The record retention schedule can be found here: http://www.sec.state.ma.us/arc/arcpdf/0211.pdf
  - Please consult ISIS
- Documents with CI must be shredded using a shredder that is of commercial quality and has a crosscutting feature before disposing of them
  - shredding must be conducted by persons authorized to view the confidential information
- Documents containing CI that are waiting to be shredded must be stored in a secured area and clearly marked as confidential

Privacy Incidents and Data Breaches

Security Breach

A breach is the use of or disclosure of protected health information in violation of program policies and job responsibilities

Reported Breaches

- Types of breaches nationally (in order of # of occurrences): loss/theft of laptops, loss/theft electronic portable devices, loss/theft paper documents, unauthorized access/disclosure via internal release of documents (email most common), unauthorized access/disclosure via hacking, improper disposal of documents
- Insider negligence continues to be the root of data breaches in 42% of cases

Staff Responsibilities

- It is the responsibility of all volunteers and staff to report a suspected privacy incident immediately to the team lead and the Director of ISIS
- The team lead, PIH and Director of ISIS are responsible for investigating suspected incidents in coordination with the Privacy Office / PDAO

Confidentiality Agreement

Please electronically sign in the appropriate section during the application process with PIH.

I, _____, as a person with access to confidential information _____ agree to abide by the security and confidentiality rules of the Massachusetts Department of Public Health and the Bureau of Infectious Disease and Laboratory Sciences (BIDLS), in accordance with the 105 CMR 300.120 and CDC, NCHHSTP Data Security and Confidentiality Guidelines.

With this signature, I agree to the above statement.

_____

Name: _____

Affiliation: _____

Date: _____