Ensuring Privacy and Confidentiality While Protecting Public Health
Objective

- These slides describe the standards for protecting the privacy and confidentiality of the information that held in the Massachusetts Virtual Epidemiologic Network (MAVEN), the Commonwealth’s infectious disease surveillance and case management system used for COVID-19.

- All MAVEN users are responsible for complying with the policies and procedures set forth in this training in addition to their organization’s policies and all applicable law.
Purpose

• Our work for case investigation and contract tracing 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.
Trust is Key

• Individuals share information with us in order to protect public health.
• We need people to fully disclose information in order to effectively protect public health.
• When people entrust us with their information, they count on us to ensure that it is protected properly.
• We are ALL responsible for maintaining this trust!
Our Responsibilities

Maintain the trust of the public by:

- Ensuring compliance with applicable state and federal laws by following policies and protocols about data security and privacy at all times
- Ensuring that Confidential Information is protected and appropriately secured at all times
- Accessing Confidential Information only on a need-to-know basis
- Reporting any known or suspected Privacy Incidents to DPH
Working With Confidential Information (CI)
Broadly, **Confidential Information** (CI) is any individually identifiable information, including, but not limited to, medical and demographic information, that: (1) reveals the identity of an individual or is readily identified with an individual, such as name, address, telephone number, social security number, health identification number, or date of birth; or (2) provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify an individual.
Examples of Confidential Information

- **Individual identifiers** – such as names and addresses of cases and contacts
- **Identification numbers** – such as social security numbers, MAVEN IDs, or medical record IDs
- **Clinical information** – such as diagnoses, test results, symptoms, or underlying health conditions
- **Demographic information** – such as race, ethnicity, religious affiliation, or political affiliation
- **Household information** – such as risk factors, living situation, or services needed/received
Confidential Information (Cont’d)

• Note that information may still be identifiable even if names, dates of birth, or other pieces of data are removed.

• Sophisticated techniques exist to re-identify individuals based on information that may not seem to be identifiable at first glance.

• If you have questions about whether information should be treated as confidential, ask DPH.
The following should never be documented in MAVEN as part of your work for case investigation:

• Information relating to HIV status
• Mental health diagnosis/substance use information
• Health insurance ID number
• Social security numbers
• Immigration status
• Bank account/financial account information
• Drivers license/state identification number
Access to CI

- Individuals working on behalf of institutions of higher education as part of case investigation of COVID-19 cases within their community are only authorized to access the minimum amount of CI within MAVEN needed in order to fulfill their job responsibilities.
- Individuals are granted access to CI based on their roles and job responsibilities.
- Access to CI must be limited based on what is required to fulfill responsibilities.
- Individuals who have access to information in MAVEN are not authorized to search for information on individuals not directly related to their job responsibilities.
Working with CI

- CI must never be stored in an unsecured location, including but not limited to on personal devices, AT ANY TIME OR FOR ANY PURPOSE.
  - This includes downloads, exports, copy/paste, screenshot, or otherwise stored on a personal devices (including laptops, phones, and tablets)
- CI may never be transmitted via unsecured email, text, or chat.
Examples of prohibited storage or transmission of CI:

- You may not save any MAVEN reports or any report that contains MAVEN IDs or personal information on your personal computer at any time for the purpose of attaching it to an email, uploading it to the cloud or for any other reason.
- You may not use MAVEN IDs in Chat or unsecured email.
- You may not store tracking lists, referral lists or any other documents containing MAVEN IDs, CTC IDs or Confidential Information on your personal computer at any time.
Working Remotely

• When working remotely, Confidential Information must be accessed only in accordance with the approved procedures provided to you by your employer.

• Remote work stations should be set up so that conversations may not be overheard and computer screens and any paper CI may not be seen by others.

• Ensure that the remote workstation is as secure as possible.

• To the extent you are permitted to work with CI in paper form, it must be locked away or otherwise secured when not in use.
• Staff who work on personal devices should run security software, such as Antivirus software, on their workstations as a best practice
• Staff who work on personal devices should keep software (such as OS and browsers) up to date.
• Encrypt home networks whenever possible.
• Change the default credentials of network devices whenever possible.
• Beware of Phishing schemes:
  – Check domain names when internet browsing
  – Ignore suspicious requests for financial or health care treatment information
  – Make note of email addresses and other markers of an organizational authenticity
• If you take notes on paper while at work:
  – They must be secure throughout the day and not observable to any other staff
  – You must shred all papers at the end of every shift
  – You may not maintain any paper notes
• You cannot take notes that contain CI electronically on your personal computer or any other device for work.
  – Why? It would violate the prohibition on storage of Confidential Information on personal devices or computers.
Discussing CI Via Telephone

- Calls discussing CI must be made in a secure area where conversations may not be overheard.
- Individuals conducting CI must be reasonably certain that the person you are speaking with is the person you intended to reach.
- Share the minimum amount of CI to accomplish the surveillance or epidemiological objective of the call.
- Follow all relevant protocols when setting up outgoing voicemail messages or leaving voicemails while working.
- If conducting CI on a personal phone, must clear or delete all recent calls to cases or contacts from the phones at the end of a shift.
Disclosure of CI

• Staff are prohibited from disclosing Confidential Information (including any personal information) to anyone, except for authorized CTC or DPH staff.
• When discussing CI with authorized staff members, only disclose it to staff members who need it to perform their work duties, or who are assisting you with yours.
• Only disclose what is necessary for work to be accomplished.
• Staff are prohibited disclosing or otherwise discussing any of their work on any social media platforms, including but not limited to Facebook, Twitter, Instagram, TikTok, etc.
Privacy Incidents
A privacy incident is the use of or disclosure of Confidential Information in violation of the policies and procedures set forth in this training.

Examples of privacy incidents include:
- The use or disclosure of CI, whether inadvertent or intentional, beyond what is needed for work to be completed
- The theft or loss of paper documents, a laptop, thumb drive, or other device containing CI
- Unauthorized access of CI via hacking or other mechanism
Reporting Privacy Incidents

• All MAVEN users must immediately report any suspected privacy incidents to DPH.
• If you are conducting contact tracing under a delegation of authority from your Local Board of Health (LBOH) privacy incidents should also be reported to the LBOH
• There is no retaliation for the good faith reporting of privacy incidents.
• You must treat all electronic data related to your job confidentially.
  – You may not acquire access to CI unless such access is required by your work, and may not disseminate CI that you have rightful access to, unless such dissemination is required by DPH.
MAVEN Security

• Never share your MAVEN password with anyone, and promptly notify DPH if you suspect that any of your passwords have been compromised.

• Do not store any MAVEN data on a personal computer, laptop, cell phone or in paper records.

• If you take notes on paper during your work, you must shred them immediately after your shift.
Thank you for completing this training. Before you can be granted MAVEN access, you must sign the attestation available here.