Information Privacy & Security Training

For:

Community Rapid Testing Program

Presented by:

California Department of Public Health

June 2023

Privacy and Information Security Topics

This training will address the following:

- Information Classifications
- Information Privacy
  - State and Federal Privacy Laws and Standards
  - Minimum Necessary
  - Use and Disclosure of PHI & PII
- Information Security
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
- Information Security Incidents and Privacy Breaches
- Penalties

Information Classifications

Information Classifications

All information is not created equal. For purposes of information security and privacy, Testing Program information could be classified as:

- **Personally Identifiable Information (PII) –** This is information that identifies or describes an individual. Examples include name, date of birth, Social Security number, financial account number, individually identifiable health information, race, gender, COVID-19 test results, etc.
- **Confidential Information** – Information only authorized persons can have access to. This is information maintained by the Testing Program that is *exempt from disclosure*. Examples include communications with legal counsel.
- **Public Information** – Information about the Testing Program and its services that can be shared with everyone. *A determination as to whether information is public may only be made by CDPH management or the Office of Legal Services.*

Most **Confidential Information** you will access is considered **Personal Information**.

If you are not sure if information is confidential, treat it as such until informed otherwise by CDPH management or the Office of Legal Services.

Information Privacy

Information Privacy

- Privacy concerns exist wherever and whenever **Personal** or **Confidential Information** is collected, stored, or disseminated. Privacy is a concern whether the information is electronic, oral, or physical.

- Information privacy issues can arise from a wide range of sources, including information collected in Primary, or while testing individuals.

- The challenge in information privacy is to collect, store, and share information related to COVID-19 testing while protecting **Personal** and **Confidential Information**.

State and Federal Privacy Laws and Standards

- Privacy laws and standards are found at the federal, state, and local levels.

- CDPH's Testing Program is primarily governed by the Information Practices Act (IPA) (California Civil Code section 1798, et seq.) and state policy (State Administrative Manual section 5300).

- The Testing Program is not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, your organization and some of the information you hold might be!

- The takeaway is, regardless of whether the information is covered by the IPA, HIPAA, or the Family Educational Rights and Privacy Act (FERPA), the privacy and protection of **Personal** and **Confidential Information** is of the utmost importance!

Information Practices Act

- The Information Practices Act (IPA) establishes requirements for all state agencies for the collection, maintenance and dissemination of **personal information**.
- The IPA was established in 1977 and is a state law to protect **personal information**, including medical information.
- **Remember – medical information includes (but is definitely not limited to!) both positive and negative COVID test results and whether someone is vaccinated.**
- The IPA requires that **personal information** is kept confidential.

Personal Information Under The IPA

- **Personal information** (PII) is any information maintained by an agency that identifies or describes an individual. Some examples include:
  - Name
  - Social Security number
  - Medical information, or information that implies a medical condition
  - Financial information (account number, debit, or credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account)
  - Driver's license number or California identification card number
  - Health insurance information (can include date of birth)
  - Statements made by or attributed to the individual
  - Home address
  - Home telephone number

HIPAA Overview

- HIPAA is a federal regulation that protects the confidentiality and security of **protected health information (PHI)**. HIPAA includes both privacy and security standards.
- HIPAA creates and protects individual privacy rights for **PHI** and governs the use and disclosure of that information.
  - **PHI** is “individually identifiable health information” in any form or media, whether electronic, paper, or oral that relates to:
    - The individual’s past, present or future physical or mental health or condition, or
    - The provision of health care to the individual.
- When there are stricter state or federal laws for a specific program regarding use and disclosure of **PHI**, those stricter laws must be followed.
- The next slide explains why we’re talking about HIPAA when the IPA governs the Testing Program.

HIPAA Overview Cont'd

- As noted above, the CDPH Testing Program is not governed by HIPAA.
- The CDPH Privacy Office has performed an analysis of the services provided by the Testing Program and determined they do not fall under the definition of a "covered program" set forth in HIPAA. Therefore, HIPAA does not apply.
- However, several concepts within HIPAA such as PHI (discussed above) or minimum necessary (discussed below) are concepts you need to understand so that you can effectively use, maintain, and help CDPH control the improper sharing of personal information of individuals.

PII vs. PHI

- Personally identifiable information (PII) and protected health information (PHI) may seem similar on the surface, but key distinctions set them apart.
- While PII is a catch-all term for any information that can be traced to an individual's identity, PHI applies specifically to HIPAA covered entities that possess identifiable health information.
- PII includes, but is not limited to, Social Security numbers, passport numbers, driver's license numbers, addresses, email addresses, photos, biometric data, or any other information that can be traced to one individual. Medical, educational, financial, and employment information all fall under PII.
- Because many Testing Program partners may have access to both PHI and PII, all data is treated the same to streamlines processes.

Minimum Necessary

Minimum necessary is a concept to ensure **PHI** is limited in its use and disclosure to minimize security risks. Access to **PHI or PII** must be limited to the smallest amount necessary to do your job, including:

- **Requesting the minimum amount of information necessary**
- **Using the minimum amount of information necessary**
- **Disclosing the minimum amount of information necessary**

Minimum Necessary Cont'd

- **IMPORTANT REMINDERS**:
  - When submitting a technical assistance request to CDPH or Primary.Health, send only the minimum necessary information to convey your concern.
  - **QR codes** on the BinaxNOW test cards are used to identify individuals and protect PII
  - **Do not** include any personal information on the test cards, texts, or emails, including name, DOB, or screenshot containing PII.

Minimum Necessary Cont'd

Remember, if in doubt, ask the CDPH Testing Program site coordinator if you are uncertain if the disclosure is permissible.

Internal Sharing of PII

- Only share **PII** with other individuals in the Testing Program if they require it for their operations.
- **PII** may be shared with internal business associates when assisting operations, ex. Legal, accounting, audits, and investigations.
- **NEVER** forward or share Social Security numbers.

Uses and Disclosures of PHI & PII

- **Use** is the sharing, application, utilization, examination, or analysis of **PHI** and **PII**.
- **Disclosure** is the release, transfer, provision of access to, or divulging in any other manner of **PHI** and **PII** outside the program holding the information.
- Everyone must ensure **PHI**, **PII**, and **Confidential Information** is not released to external entities in violation of federal or state laws/regulations, or CDPH policies.
- If a testing site is asked to disclose personal information to individuals other than to whom the information pertains, and they or their managers are concerned about the disclosure, they are to immediately contact CDPH at CommunityRapidTesting@cdph.ca.gov and the Privacy Office at privacy@cdph.ca.gov for further guidance.

- **Non-routine releases of data must be approved by the CDPH Privacy Officer and the Information Security Officer in writing.**

Disclosing PHI & Personal Information

- **Rule of Thumb**: Do not disclose any **PHI** or **PII** to any external entity unless approved by CDPH.
  - "External entity" is any individual to whom the personal information does not pertain.
    - This includes fellow staff who are not part of the Testing Program or who do not have a business-related need to access the information.
  - Consult with your manager before you disclose any such information, or when you have any questions.
  - If unsure, do not attempt to make a determination if the information can be shared. Please consult with your manager.

- **Common Required Disclosures:** There are instances when disclosure of **PHI** or **PII** is required, including:
  - To the individual to whom the record pertains; or to the parent, guardian, conservator, or authorized representative
  - With prior written voluntary authorization/consent

Information Security

Administrative Safeguards

Administrative Safeguards include documented policies and procedures for day-to-day operations; managing the conduct of staff; accessing the State's automatic information systems and related devices; and managing the selection, development, and use of security controls.

Physical Safeguards

- **Physical Safeguards** are security measures meant to protect electronic information systems, and confidential information (in any form); as well as related buildings and equipment from natural hazards, environmental hazards, and unauthorized intrusion. When authorized to work remotely, physical safeguards are similar to protecting your own home or possessions.
- Some examples of physical safeguards are:
  - Identification for all employees and visitors
  - Locked desk drawers, cabinets, rooms and buildings
  - Locking doors and windows when not home
  - Shredding of confidential information
  - Using caution when printing, faxing, and mailing
  - Protecting mobile computing devices from theft and misuse

Unattended Areas

- You should **never** leave **personal** or **confidential information** *unattended*, where unauthorized individuals may access it, even for a few minutes, including during working hours.

- Another individual who is authorized to see the information may watch your personal or confidential information if they are in the immediate area.

Securing Information

- **Personal and confidential information** MUST be secured during non-working hours, even if the building is secure. For example:
  - Put documents in a locked drawer or a lockable filing cabinet.
  - Do not leave personal or confidential information unsecured in your office, unless your office is locked.
  - Do not leave personal or confidential information visible on top of or under your desk.
  - Do not leave keys to cabinets, drawers, or office doors in a desk or any obvious place.
  - **REMEMBER**: This includes your desk and office at home if teleworking!

Securing Information Cont'd

- Paper documents are at a higher risk than electronic files of being breached because they cannot be encrypted.
  - **Never** print documents or take paperwork offsite unless absolutely necessary.
  - **Never** take handwritten notes unless absolutely necessary.
  - Documents must be shredded or placed in a locked confidential destruct container as soon as possible when no longer needed.
  - Work related documents should be kept separate from any personal documents.
- When left unattended, secure information and/or documents in locked cabinets, locked drawers, or locked rooms. **Do not** leave information unattended in vehicles or other locations where it may be viewed or stolen.

Confidential Destruct

When you no longer need the **personal or confidential information** for business purposes, you have a few options to dispose/destroy this information.

- **Physical Documents**
  - Immediately shred the documents yourself.
  - Utilize locked, confidential destruction bins.
- **Electronic Documents**
  - Perform a secure deletion or wipe of the information.

Do not discard **personal or confidential information** at home, away from your department or in recycle bins/waste baskets unless shredded. If you do not have a shredder, do not create paper documents.

Confidential destruct documents are not to be stored in boxes in employees' cubicles or offices.

Emailing/Texting Personal or Confidential Information

- Verify all recipients' email addresses/mobile numbers before sending.

- If you discover that you sent the email or text to the wrong email address, please immediately report the incident to your supervisor and have them report the incident to the privacy and security office if the email or text contains PHI or PII, so that the privacy attorney can make a determination as to whether a breach notification letter needs to be mailed out to the individual(s) potentially affected. Forms can be provided by the privacy office.

Safeguards for Verbal Communication

- Take reasonable steps to protect the privacy of all verbal exchanges or discussions of **personal** or **confidential information**, regardless of where the discussion occurs.
- Find enclosed offices to discuss **personal** or **confidential information**.
- Do not discuss **personal** or **confidential information** with family or friends.
- Do not discuss **personal** or **confidential information** with those who do not need to know for a valid business purpose even if they work with you.
- Verify the identity and authority of persons with whom you verbally exchange information.
- Do not discuss an individual's **personal** or **confidential information** with the individual's family, friends.

Security of Mobile Devices

- Mobile devices include laptops, tablets, PC Notebooks, USB storage devices, flash memory, and cell phones.
- If you are utilizing your own mobile device for Testing Program purposes, ensure it is password protected or encrypted in some manner.
- When taken off the worksite premises (which includes your home if you are authorized to work remotely), mobile devices must not be separated from employees at airports, in cars, hotel rooms, etc.
- When mobile devices are taken off worksite premises:
  - Do not leave mobile devices unattended.
  - When not being used, secure all mobile devices.
  - Cable lock a laptop to an immovable surface.

Technical Safeguards

- **Technical Safeguards** are security measures that specify how to use technology to protect the information gathered, stored, and transmitted, particularly by controlling access to it.

Email Security

- Always check email addresses to ensure delivery to intended recipient(s).
- Do not forward PHI or PII to a personal email account.
- Do not send email messages containing **personal** or **confidential information**, even if it is to another governmental entity email address

Email Security cont'd

- Insert a confidentiality statement at the end of your email.

- Example of a confidentiality statement:
  - *CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication. Your receipt of this message is not intended to waive any applicable privilege.*

Passwords

- You are responsible for the confidentiality and security of their passwords. You should:
  - Change the password at least every 60 days, or sooner if you suspect it has been compromised.
  - Not share or write down your password.
  - Not include your password in a data file, log-on script, or macro.
- Create a “strong” password by avoiding common references like your significant other’s name, pet’s name, birthday, favorite color, sequential numbers/digits (abc, 123, 5555), easy to guess, etc.
  - Do not use a word in the dictionary.
  - Have a unique password for each logon, and don’t use the same password for multiple systems.
  - Use a password with an odd number of characters, at least nine digits long, with at least:
    - One upper case letter and one lower case letter
    - One number
    - One unique character such as !@#$%^&*()

Report any suspected unauthorized use of a password to your supervisor and CDPH immediately.

Computing Equipment

- Use Ctrl-Alt-Delete, Windows-L, or a lock key to lock your computer screen before you leave it unattended.
- Store files on a server or shared drive because they are backed up. Do not store information or files on desktops.
- Do not use computer equipment for any unauthorized purposes.

Mobile Computing Devices

- Do not download or store **personal** or **confidential information** to mobile devices unless you have written permission to do so. If permitted only download or store the minimum amount of **personal** or **confidential information** necessary on mobile devices.
- Do not access Primary.Health or other Testing Program platforms from your mobile device unless you are at your testing site or a designated work area.
- Make sure that you always log out of all Testing Program platforms when not actively using them.
- **NEVER** download or store SSNs on mobile devices.

Don’t Be the Weakest Link!

- Historically, state departments and their contractors have had breaches involving loss or theft. **Be vigilant with state-issued computers or mobile devices or any computer or mobile device on which state work is conducted.**
  - Do not download personal files onto state-issued computers or mobile devices.
  - Do not check home email accounts on state-issued computers or mobile devices.
  - Do not use unsecured wireless networks.
  - If you have a blog, social network website, etc., do not post any **personal** or **confidential information** Testing Program information on it, including when you are at home.

Remote Access

Remote Access

- Remote access involves using an externally located computer (e.g. home, hotel) to access Testing Program email, documents, and applications.
- Remote access is most commonly used after hours, when traveling, or when teleworking/working from home.
- You should not access Testing Program information remotely unless you have been approved to do so by the Testing Program.

Risks and Concerns of Remote Access

- Areas of concern include:
  - Lost or stolen media, devices, or paper documents
  - Improper disposal of media and paper documents
  - Malicious software on personal computer that steals information
- Inappropriate exposure or disclosure of **personal** or **confidential information** to others, such as visitors to your home, which may trigger state or federal breach notification laws.
- Violations of Testing Program policies may also lead to disciplinary action and termination from the Testing Program.

Download Dangers

- Minimize downloading or taking any Testing Program **personal** or **confidential information** from the test site.
- Do not download Testing Program **personal** or **confidential information** onto personal computers or mobile devices. This includes transferring information via flash drives, CDs, etc.
- Do not email or post Testing Program **personal** or **confidential information** to personal email accounts, social media or other non-Testing Program applications, media or systems.
- Do not email screenshots with PII/PHI to anyone, including CDPH employees.
- If uncertain what is permissible, consult with your immediate supervisor and CDPH.

Computer Security

Personal computers generally do not have all the protections against malicious software that your state computer has. If available, use of a department-issued and managed laptop is recommended if you are accessing personal or confidential information via remote access.

- If using a home computer for remote access, ensure it has:
  - Antivirus software that is current and configured to update at least daily
  - Security patches installed monthly
  - Software or hardware firewall installed
- For personally-owned computers, setup automatic installation or notification of security patches, and ensure you update software such as Adobe Acrobat and your internet browser on a monthly basis.
- Do not use unsecured, open wireless networks.
- If you suspect someone viewed your password or watched you type it in, immediately change your password.

Do not forget to lock your screen while away from computer, even when working from home!

Computer Security Cont'd

- Do not trust any individual who claims authority to access your information or password. Passwords should never be shared.
- Do not click on links or attachments in emails unless you are expecting the email or can validate it is authentic. Do not click on links unless it's work related and necessary to do so… the website may be fake.
- Remote Access security controls and policies protect Testing Program information and avoid State and Federal law violations. Ignoring, disabling, or working around security and privacy controls or policies can be grounds for disciplinary action and termination from the program.
- Do not allow a private technical support organization to take remote control access of your PC or laptop logged in to Testing Program information portals.
- If a breach of security is suspected, immediately report it to CommunityRapidTesting@cdph.ca.gov and the CDPH Information Security Office (CDPH.InfoSecurityOffice@cdph.ca.gov).
- If you suspect Testing Program personal or confidential information was viewed by an unauthorized individual, notify CommunityRapidTesting@cdph.ca.gov and notify the CDPH Privacy Office (Privacy@cdph.ca.gov).

Information Security Incidents and Privacy Breaches

Information Security Incidents

- An **information security incident** is an actual or suspected occurrence of damage, destruction, unauthorized access or disclosure of equipment or information. This includes theft, attempted theft, or loss of equipment or devices with PII or PHI on them (laptops, cell phones, etc.); or information as well as fraud, misuse or inappropriate use of State property. Additionally, detection of a computer virus or hacking on a State computer is also considered an incident.
- **Simply put**: theft or loss of any Testing Program information, equipment, or device is a security incident and must be reported to the CDPH Information Security Office (ISO) immediately.
- The ISO will determine if the computer contained **personal** or **confidential information**. If any such information was present, the incident may also be classified as a privacy breach.
- When a privacy breach is suspected, the ISO will then escalate to the CDPH Privacy Office. While information security incidents and privacy breaches are similar, there are differences in the escalation process and reporting requirements.

Reporting Security Incidents

CDPH has a specified notification and reporting processes when information security incidents occur. As soon as you are aware an incident has or may have occurred, report it to your manager/supervisor, who will notify the necessary people.

Report the following information to your manager/supervisor:

- Your name and title
- Testing Program site you are assisting
- Your contact phone number
- Your physical address

In addition, as applicable to the incident, you must report:

- The IT equipment or device lost or stolen
- Description of the information disclosed or accessed by an unauthorized person
- Date the incident was first discovered and date when action was taken
- How the incident was carried out, if known
- What evidence is available to assist in the investigation and who may have additional knowledge
- A police report number, if any State equipment was stolen

Reporting Security Incidents Cont'd

Your manager/supervisor (or designee) must immediately report the incident, and all the relevant information, to CDPH.

After it is reported, under the guidance of the ISO, your manager/supervisor will work with CDPH to complete an incident report form and a corrective action plan for submittal within 5 days. The corrective action details the steps taken by the Testing Program to mitigate or remediate the incident. Delays in reporting, handling, or putting correcting action plans in place result in escalation of damages and risk of further losses of the information the Testing Program is entrusted with.

Direct any questions regarding information security incident reporting to:

- ISO email address: CDPH.InfoSecurityOffice@cdph.ca.gov
- ISO phone via IT Service Desk: 916-440-7000 or 800-579-0874.

Privacy Breaches

A privacy breach is an unauthorized disclosure of personal information or PHI under the Information Practices Act of 1977, the HIPAA Privacy Rule, or State Policy.

Privacy breaches can be oral, paper or electronic, and occur when information is transmitted to an unintended or unauthorized recipient.

Examples of breaches include:
Verbal Breaches: Verbally disclosing **PHI/personal information** to unauthorized individuals during phone calls, in a manner not permitted by state or federal laws, which poses a significant risk of financial, reputational, or other harm to the affected individual/patient.

Paper Breaches: Misdirected paper mailers or faxes with **PHI/personal information**, loss or theft of paper documents containing **PHI/personal information**, mailings with **PHI/personal information** to the incorrect individual, or printing **PHI/personal information** on the outside of an envelope or viewable through an envelope window.

Electronic Breaches: Stolen/lost unencrypted, laptops, hard drives, PCs with **PHI/personal information**; stolen/lost unencrypted thumb drives with **PHI/personal information**; misdirected electronic fax or emails with **PHI/personal information** that were sent to unauthorized persons; unauthorized sharing of **PHI/personal information** on social media; unencrypted e-mails; password sharing; and hacking into electronic databases.

Penalties

Liability

- The Information Practices Act (IPA) states an intentional violation of the IPA by an employee is cause for discipline, up to and including termination. It is a misdemeanor to request or obtain a record with **personal information** under false pretenses and you can receive a fine up to **$5,000** and imprisonment up to one year for doing so. Even if you unintentionally violate the IPA, once the violation is discovered, and the privacy office has instructed you to cease whatever action is in violation, you must take immediate action and adhere to the request.

- **Directors, officers, and employees** may be liable for criminal penalties. It is sufficient they know the facts constituting the offense, whether or not they know the conduct was contrary to the statute or regulations.

Complaints for PHI/Personal Information Violations

- **Individuals have the right to complain about a violation of privacy or information security policies, whether they are a patient, member of the workforce, or other business associate.**

- CDPH prohibits retaliatory action against anyone filing a complaint.

- Any individual whose **PHI/personal information** is maintained by a department may file complaints regarding suspected violations of the IPA or HIPAA Privacy Rule. Other persons who can file complaints include, but are not limited to, employees, business associate employees, service recipients, advocates, lawyers, and whistleblowers.

Summary of Key Concepts

- Privacy concerns exist wherever and whenever **Personal** or **Confidential Information** is collected, stored, or disseminated. Privacy is a concern whether the information is electronic, oral, or physical.
- The Information Practices Act (IPA) establishes requirements for all state agencies for the collection, maintenance and dissemination of **personal information**.
- **Minimum necessary** Access to **PII** must be limited to the smallest amount necessary to do your job
- Only share **PII** with other individuals in the Testing Program if they require it for their operations
- Do not disclose any **PII** or **PHI** to any external entity unless approved by CDPH

Action Steps to Take in Your Workplace

- **Do not** include any personal information on the test cards, texts, or emails, including name, DOB, or screenshot containing PII or PHI.
- Take steps to protect the privacy of all verbal exchanges or discussions of **personal** or **confidential information**, regardless of where the discussion occurs.
- If you are utilizing your own mobile device for Testing Program purposes, ensure it is password protected or encrypted in some manner.
- Anytime you send email messages containing **personal** or **confidential information**, even if it is to another governmental entity email address, the email should be encrypted.
- **Simply put**: theft or loss of any Testing Program information, equipment, or device is a security incident and must be reported to CommunityRapidTesting@cdph.ca.gov and the CDPH ISO CDPH.InfoSecurityOffice@cdph.ca.gov immediately.
- **Personal and confidential information** MUST be always secured, including during non-working hours.
- **Paper documents are at a higher risk than electronic files** of being breached. Secure them!