Annual Information Security Awareness Training

Exhibit D

Chief Information Officer: Cheryl Larson

CALIFORNIA CORRECTIONAL
HEALTH CARE SERVICES

Introduction

Information security training is required by state and federal mandates. This course provides California Correctional Health Care Services (CCHCS) employees, contractors, and other personnel who have access to CCHCS information assets with the knowledge to protect the information system and sensitive data from internal and external threats.

D.A.N.G.E.R.

D: Define – What is Information Security

A: Acknowledge – Why is it important for YOU to protect information & investments

N: Notice – Recognize & notice a security threat when you see one

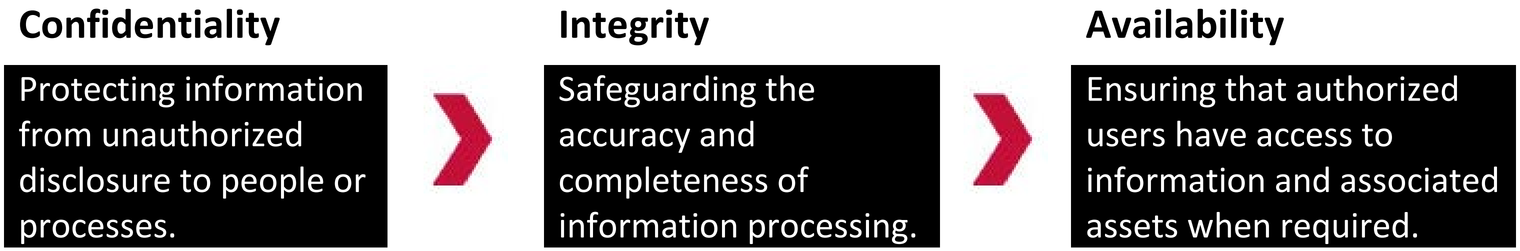
G: Guard – Take precautions to protect your information

E: Educate – Further Educate yourself about Information Security with these resources

R: Report – Report incidents

Define: What is Information Security?

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability of information.



Confidentiality

Protecting information from unauthorized disclosure to people or processes.

Integrity

Safeguarding the accuracy and completeness of information processing.

Availability

Ensuring that authorized users have access to information and associated assets when required.

Define: What is Information Security?

Privacy: A set of fair information practices to ensure that an individual's personal information is accurate, secure, and current, and that individuals know about the uses of their data.

Personally Identifiable Information (PII): Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains.

Protected Health Information (PHI): Protected health information is defined as any information, in any form that relates to the past, present, or future physical or mental health or condition of an 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; and that can be used to identify an individual.

Health Insurance Portability and Accountability Act (HIPAA): Describes a list of specific direct identifiers that, along with a name, constitute individually identifiable information. If you have any one of these direct identifiers in your health information dataset, along with a name, you have PHI, and must be safeguarded appropriately.

Example: PHI could be a name with information regarding his/her Medi-Cal status.

Direct Identifiers

- Name
- Address – street address, city, county, zip code, or other geographic codes
- Dates directly related to patient (except year), including DOB, admission or discharge date
- Telephone and/or FAX Numbers
- Driver’s License Number
- E-mail Addresses
- Social Security Number
- Medical ID Number / CIN
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number, including license plates
- Web Addresses (URLs)
- Internet Protocol Address
- Photographic Images
- Any other unique identifying number, characteristic, or code

Acknowledge: Information Security is YOUR Responsibility

CCHCS employees are granted access to Internet and E-mail resources to provide education, research, marketing, procurement, and service opportunities in the performance of their duties.

Conduct all Internet and/or e-mail activities in a professional, lawful, and ethical manner. This includes the development of content of the Internet.

Accessing a personal or private Internet Service Provider for personal use while using any state equipment, or using non-state equipment for conducting state business, does not release an employee from the responsibility of complying with this policy.

Be aware that all employee computer activity is logged and monitored, all computer usage has an audit trail. Employees shall have no expectation of privacy for their use of department equipment.

CCHCS employees are granted access to information systems to perform their job functions on a need to know minimum necessary basis. If you feel you have access to “too much” information, speak to your supervisor.

Consequences

Organizational Consequences:

- Legal ramifications including civil and criminal for CCHCS
- Loss/misuse of sensitive information
- Injury or damage for those who have had their private information exposed
- Potential financial ramifications for those affected
- Reputation damage, loss of trust for CCHCS

Personal Consequences:

- Employee disciplinary action (written warning, suspension without pay, pay reduction, demotion, dismissal)
- Civil and criminal penalties (HIPAA violations)
- Fine up to $1.5 million and/or 10 years imprisonment
- Criminal prosecution for personal use – personal benefit

Notice: Recognize & notice a security threat or incident when you see one

A threat is a potential cause of an unwanted incident that may result in harm of an organization (agency) or a person.

Virus	Social Engineering
Worm	Shoulder Surfing
Trojan	Tailgating
BotNet	Phishing/Whaling
Adware	SQL Injections
Spyware	E-mail SPAM

Cyber Attack: Malicious attacks with the intent to cause major disruptions to our everyday government operations.

The Department of Defense (DoD) detects three million unauthorized “scans” or attempts by possible intruders to access official networks every day.

Notice: Recognize & notice a security threat or incident when you see one

A Security Incident may involve:

- Unauthorized disclosure, modification and or destruction of confidential information
- Inappropriate use or unauthorized access to computer systems
- Unintentional or inappropriate release of confidential information
- Theft, loss, damage or destruction of state equipment
- Use of a state computer to commit a crime

Examples include:

- Faxes or e-mails of PHI information to incorrect providers, organizations, beneficiaries, or individuals
- Mis-sent or lost documents including any form of protected information
- Mailings of PHI to incorrect providers, organizations, beneficiaries, or individuals
- Disclosures greater than minimum necessary to perform a job
- Password sharing
- Unauthorized viewing, access, or disclosure of confidential information
- Stolen laptop
- Lost mobile phone

Social Engineering: A common technique by hackers is to attempt to trick you by posing as an administrator or other person of authority to get CCHCS network and system information.

Phishing: Spear phishing scams will often appear to be from a department's own human resources or IT support and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can steal data.

*Per the State Administrative Manual (SAM)

Guard: Take precautions to protect your information

CCHCS uses administrative, physical and technical safeguards to protect PHI, PII, Confidential, and Sensitive Information.

Administrative Safeguards: Documented policies and procedures for day-to-day operations, managing the conduct of employees accessing the state's automated information systems and related devices, and managing the selection, development and use of security controls.

Examples: Policies, disaster recovery planning, risk management, training

Physical Safeguards: Security measures for protecting the Department's tangible information systems and confidential information, as well as related buildings and equipment from environmental hazards and unauthorized intrusion and theft.

Examples: Employee and visitor identification, locked desks and work spaces, shredding confidential information, caution when transmitting data, protecting mobile computing devices.

Technical Safeguards: Technology resources implemented to protect and improve the networking environment.

Examples: Encryption, Internet content filtering, anti-virus software, security patches, computer usage audit lodging, software install approvals, screen savers.

Guard: Take precautions to protect your information

Things TO DO to protect Information

Always lock your computer when unattended (CTRL+ALT+DELETE).	Conduct all Internet and / or e-mail activities in a professional, lawful, and ethical manner.
Store files on server / shared drives that are backed up; do not store on desktops.	Secure data in your possession from unauthorized access, including family members and friends.
Keep devices on you at all times, if you must leave a device unattended, store it in a protected, locked or inconspicuous space.	When left unattended, secure data in locked cabinets, locked drawers, locked rooms.
When feasible, cable lock your laptop to an immovable surface.	Lock up confidential destruct boxes when they are left unattended.
Return IT hardware including state computers, phones, hard drives, CDs, DVDs, flash drives etc. to your local IT for the proper sanitation and disposal.	Shred documents with confidential, sensitive or personal information, including protected health information.
Always ensure delivery to intended recipient by double checking e-mail address.	Minimize downloading or taking any CCHCS data outside the workplace.
Share the minimum necessary PHI / PII / ePHI / PCI / Confidential / Sensitive Information to get the job done.	Encrypt and password protect all mobile devices.
Use a password that is at least eight digits long and include at least three unique characters (upper case letters, lower case letters, numbers and / or non-alphanumeric characters.)	Consult with your supervisor or the Information Security Office if you have any questions. CPHCS-ISO@cdcr.ca.gov.

Guard: Take precautions to protect your information

Things NOT TO DO to protect Information

Do not use state owned computer equipment for any unauthorized purposes.	Do not download CCHCS data onto non-CCHCS authorized computers or mobile devices. This includes transferring data via thumb drives, CDs, etc.
When choosing a password, avoid common references and words from the dictionary e.g., our significant other's name, pet's name, birthday, favorite color, sequential (abc, 123, 555), easy to guess, etc.	Never send e-mail messages containing ePHI / PHI / PII / Confidential / sensitive information outside of the department unless you are authorized to do so and encrypt.
Never share your password(s) with anyone. Social engineers will try to trick you in an attempt to gain access to CCHCS information systems.	Do not e-mail CCHCS data to personal e-mail or other personally owned systems.
Do not use the same password for multiple systems.	Do not leave laptops in unattended vehicles or other locations where it may be easily taken.
Never open an unexpected – unrecognized e-mail attachment.	Do not leave PHI / PII / confidential information in public locations.
Do not release PHI, PII or ePHI without prior authorization and approval.	Do not install or download unauthorized software.

Guard: Take precautions to protect your information

Computer Equipment:

- Always lock your computer when unattended (CTRL+ALT+DELETE).
- Store files on server / shared drives that are backed up; do not store on desktops.
- Do not use computer equipment for any unauthorized purposes.

Mobile Devices:

- Keep devices on you at all times, if you must leave a device unattended, store it in a protected, locked or inconspicuous space.
- Mobile devices must be encrypted and password protected.
- When feasible, cable lock your laptop to an immovable surface.

Remote Access:

- Remote Access is a method to connect to the CCHCS network from remote locations in a very secure fashion. Always protect your computer by ensuring it has the latest security patches. Plug into the network at least every 30 days.
- Remote access has been known to be the most frequent method of exposure of PHI or ePHI leading to fines and personal liabilities.

Disposal of Information or Assets:

- Return IT hardware including state computers, phones, hard drives, CD's, DVD's, flash drives, etc. to your local IT for the proper sanitation and disposal.
- Printed documents must be shredded per government regulations.

HIPAA-Protected Information:

- Do not release PHI, PII or ePHI without prior authorization and approval.
- When approved for sharing PHI, PII, ePHI, share the minimum necessary.

Educate: Further Educate yourself about Information Security with these resources

It is important to know your organization’s policies and procedures to ensure the highest level of information security.

For more information visit the following resources:

- CDCR Department Operations Manual (DOM)
- State Administrative Manual (SAM)
- The Information Practices Act
- Health Insurance Portability and Accountability Act – HIPAA – Security Rule
- Health Information Technology for Economic and Clinical Health (HITECH)
- Office of Health Information Integrity (Cal OHII)

Report: Report Incidents

If you feel there has been a threat or incident, immediately contact your manager and proceed with the following steps:

Report the incident to CCHCS Information Security Office (ISO) via E-mail CPHCS-ISO@cdcr.ca.gov and/or Telephone Number (916) 691-3242

Request and complete CCHCS Information Security Incident Form (ISIR) within (5) business days.

Information to collect:

- Date and time incident occurred, and detected
- Incident location
- General description of the incident
- How the incident was discovered
- The impact of the incident on the agency
- Type of information asset that was lost / breached (media, device, paper or electronic)
- Type of data breached / lost physical or electronic; protected / sensitive (SSN, medical record or CDC#, driver's license #, financial information, etc.)
- Corrective action plan (how this incident will be prevented in the future, and when you intend to correct the current incident.)
- Estimate cost of the incident

Submit the signed security incident form to the ISO.

HIPAA-Protected Information: If you suspect that a breach of PHI, ePHI, PII or other unauthorized release of information may have occurred immediately contact CCHCS Privacy Office at E-mail: privacy@cdcr.ca.gov or by phone Toll Free at 1-877-974-4772.

Prevent security breaches by remembering **D.A.N.G.E.R.**

D.A.N.G.E.R.

D: Define – What is Information Security

A: Acknowledge – Why is it important for YOU to protect information & investments

N: Notice – Recognize & notice a security threat when you see one

G: Guard – Take precautions to protect your information

E: Educate – Further Educate yourself about Information Security with these resources

R: Report – Report incidents

CCHCS Information Security Awareness Training Questions for External Entities

Please select one answer for each question

Question 1:
Information Security is the protection of information assets from:
a) Authorized users
b) Management
c) Untrained users
d) Hackers

Question 2:
Personally Identifiable Information (PII) contains the following identifiers:
a) Name, SSN, hometown
b) SSN, Name, DOB
c) Driver’s license #, car color, year of birth
d) E-mail address, home address, eye color

Question 3:
When you see or encounter an incident, you should contact:
a) Your Chief Executive Officer (CEO)
b) Your Chief Information Officer (CIO)
c) The Information Security Officer (ISO)
d) 911

Question 4:
You should always use the same password for all your devices because it is easy to remember:
a) True
b) False

Question 5:
You should familiarize yourself with the CDCR Department Operations Manual (DOM) because it contains our CCHCS Information Security policy:
a) True
b) False

CALIFORNIA CORRECTIONAL
HEALTH CARE SERVICES

Information Security Awareness Training

I hereby attest that I have read and understand the information provided to me regarding Information Security

_______________________________ County

_______________________________ Phone Number

_______________________________ Name - Printed

_______________________________ E-mail

_______________________________ Signature

_______________________________ Date