UNDERSTANDING ARTICLE 14 FOR HHSA CONTRACTORS

Angie BC DeVoss, CHC, CHPC

County of San Diego

Health and Human Services

OBJECTIVES

- Updates to State and Federal Requirements
- Definition of Protected Information
- Encryption
- Contractor FAQs
- Privacy Incident Reporting

UPDATES

- Health Insurance Portability & Accountability Act (HIPAA)
- California Medical Information Act (CMIA)
- 42 CFR Part 2
- CA Welfare and Institutions Code (10850, 827, 15633)
- Social Security Administration Agreements
- State Agreements

UPDATES

- Changes to Federal law and increased regulations from State require changes in our day-to-day business
- Most of the new requirements simply provide more specificity to things your already do.

Old Definition	New Definition
"Protected Health Information"	"Protected Information" – includes: • Protected Health Information, • Personally Identifiable Information; • Personal Information; and • Medi-Cal information
"Business Associate" narrowly defined	Article 14 applicability expanded by State and federal governments
County responsible for County Privacy	County has increased responsibility for Contractors' Privacy
Reporting to Feds	Reporting to State and Feds

PROTECTED INFORMATION

14.1.2.7, 14.2.2.5, and 14.2.2.6

- Names
- Photographs
- Phone and Fax Numbers
- Dates (may even include year)
- Social security numbers
- Geographic subdivisions smaller than a state
- Electronic mail (email) addresses
- Web URLs/IP addresses
- Numbers related to: medical records, health plans
- Certificate/license #s
- Identifiers re: vehicles, devices, biometrics
- Other identifying numbers, codes
- Health/medical info
- Info related to public assistance benefits

PROTECTED INFORMATION

- Computers
- Client Charts
- Client Sign In Sheets
- Copies of Photo IDs and Insurance Cards
- Anasazi and SanWITS case numbers
- Voicemails
- Text Messages
- Copy Machine hard drives
- Call Logs from a Cell Phone
- Cameras

ENCRYPTION

Encryption

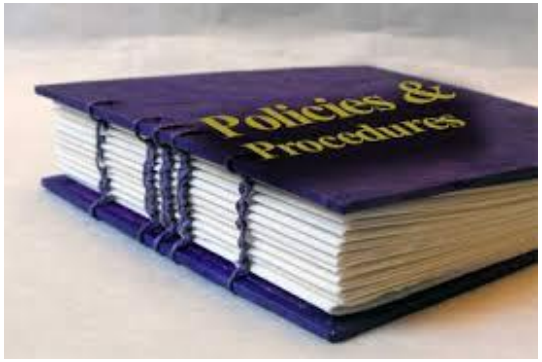
14.3.3, 14.3.3.1.1, 14.3.3.5, and 14.3.3.10

At Rest	Solution
Files on a Computer	Encrypt hard drive
Files on a smart mobile device	Encrypt mobile device
Files on a copy machine or fax	Encrypt hard drive
Flip Phones	Typically cannot encrypt; don't use for client data
In Motion	**Solution**
Emailing from encrypted computer	Email encryption software
Emailing or texting from smart mobile device	Email and/or text encryption software
Emailing from a copy machine	Encryption software for the copier
Faxing/Phones	Nothing – Good as-is

- Encryption is not the same as Password Protection

CONTRACTORS' QUESTIONS

1. Where can I get sample Privacy policies and procedures? Sample Privacy and Security Trainings? A Privacy Firm or Consultant? (14.3.1.2)
   - Internet
   - County PNPs
   - Other Contractors
   - Office of Civil Rights website
   - California DHCS Website



2. What is a security risk assessment? Is this done by an IT company? (14.3.4.1)
   - Health IT Gov

3. Who is allowed to be a Privacy and/or Security Officer? (14.1.3.11 and 14.2.3.10)
   - Anyone with enough authority to perform the duties
   - Does not have to be their "entire job"
   - One person can serve both roles

CONTRACTORS' QUESTIONS

4. What does "FIPS 140-2 certified algorithm" mean? (14.3.3.1, 14.3.3.5, 14.3.3.10)
   - National Institute of Technology Standards
   - Your IT Staff or contractor should be able to address this for your specific IT assets

5. How do I buy encryption for a smart phone, a desktop, email, or copiers? Which brand do I buy? (14.3.3.1, 14.3.3.5, 14.3.3.10)
   - There is no single type or brand of encryption, nor will every type of encryption work for every type of device.
   - For instance, the County uses Symantec for its computers, Cisco for its email, and often encryption provided through phone companies for mobile devices.

6. What is a computer warning banner? Where do I get one? (14.3.3.9.2)
   - A computer warning banner can take many different forms. There is no single standard, other than the required language, as stated in Article 14.
   - Many agencies choose to build their own banner as part of their initial login
   - Often, additional software is not required; it's simply a setting change

CONTRACTORS' QUESTIONS

7. Do all staff have to wear badges? What if it's a small office? (14.3.2.3)
   - Badges are required anywhere that contains PI

8. What is meant by "escorting visitors"? Do we have to escort our own staff if they work at other sites? Our COR? Clients? (14.3.6.2, 14.3.2.4.1, 14.3.2.6)
   - Escorting is required in spaces that contain unsecured PI.
   - Escorting is especially important for individuals not bound by Article 14
   - Each worksite is different and will likely require a different escort plan

9. How do I know which subcontractors need Article 14? (14.1.3.6)
   - Our Article 14 Decision Tree is available online

10. How do I know whether my cleaning crew is following these standards? How do I know whether my computer program meets these requirements? (14.1.3.6)
    - What does your contract with them say?

CONTRACTORS' QUESTIONS

11. Do I have to use the County's Notice of Privacy Practices? (14.1.4 , 14.1.3.3.1)
    - No, you can use your own, as long it complies with state and federal requirements.
    - Office of Civil Rights has NPP template available online
    - If you use the County's Notice of Privacy Practices, remove our logo and contact information and replace with your own

12. Do I have to have versions of my NPP available in all threshold languages?
    - Yes, due to state requirements

13. How do I log accounting of disclosures? (14.1.3.8.2, 14.2.3.8)
    - Most computer systems (like Anasazi) log everyone who touches a client's electronic file.
    - Generally, you only need to keep track of who touches a client's paper file outside of your agency. This can often be done by keeping a copy of the other entity's request for information in the client's file.
    - There are sometimes other exceptions to the accounting of disclosures for things like health care operations

CONTRACTORS' QUESTIONS

14. What kind of locks are required for client's paper charts? (14.3.2, 14.3.2.7)
    - There are no specific lock types
    - A general good rule is "two locks," such as an office door lock and locking file cabinet drawer

14. If a client requests them, can staff send texts to clients? Can they send unsecured emails?
    - HIPAA affords clients the right to request alternate communications. The County requires clients put these requests in writing.

16. What kind of security system is needed for my site? (14.3.2.5)
    - A security guard or 24-hour monitored alarm system is typical for OP clinics
    - For locations that have staff onsite 24-hours a day, no additional staff may be needed
    - We are looking at other security system options

CONTRACTORS' QUESTIONS

17. How does Article 14 apply to BYOD policies (bring your own device)?
    - Once PI is accessed by/stored on/sent from these devices, they then must follow Article 14

18. Can I leave client files in the trunk of the car during home visits? (14.3.2.7, 14.3.6.1)
    - Files must be taken with staff and cannot be left in the car, not even the trunk
    - Files also may not be "bag checked" onto commercial flights

19. What if my staff is going somewhere that does not allow them to bring anything in with them?
    - Extreme cases must be considered on a case by case basis. However, minimizing the amount of PI a worker carries with them is always important. Some helpful hints include:
        - Using client initials instead of names
        - Putting everything possible on an encrypted laptop or phone

20. What kinds of things will my COR monitor regarding Article 14?

- Your COR will monitor Article 14 just as s/he monitors the rest of your contract. S/he may choose any portion of Article 14 to monitor.
- These are some areas that have been discussed with regards to monitoring:

- Notice of Privacy Practices (14.1.4.1)
- Annual security risk assessment (14.3.4.1)
- On-Site Security System (14.3.2.5)
- Policies and Procedures, such as:
  - Privacy Incident Notification (Section 14.1.3.10 and 14.2.3.9)
  - Privacy and Security Program (14.1.3.3.2 and 14.2.3.3.2)
  - Client's requests for their file (14.1.3.9)
  - Accounting of Disclosures (14.1.3.8.2)
  - Disaster Recovery (14.3.5)
  - Visitors (14.3.6.2)
  - Computer passwords (14.3.3.6)
  - PI in cars and airplanes (14.3.2.7, 14.3.6.1)
  - Auditing (14.3.4.2)
  - Shredding (14.3.6.3)

- Computer warning banners (14.3.3.9.2)
- Background checks (14.3.1.1)
- Badges (14.3.2.3)
- Appointment of a Privacy and/or Security Officer (14.1.3.11 and 14.2.3.10)
- Subcontracts' inclusion of Article 14 language (14.1.3.6 and 14.2.3.6)
- Verification of staff's Privacy and Security training (14.3.1.2)
- Privacy Incident Follow-Up:
  - Submission of Reports on Time (14.1.3.10 and 14.2.3.9)
  - Staff sanctions (14.3.1.3)
  - Corrective Action Plan (14.1.3.10.3, 14.1.3.10.5, 14.2.3.9.3, 14.2.3.9.5)
  - Client Notifications (14.1.3.10.6.1, 14.2.3.9.6)

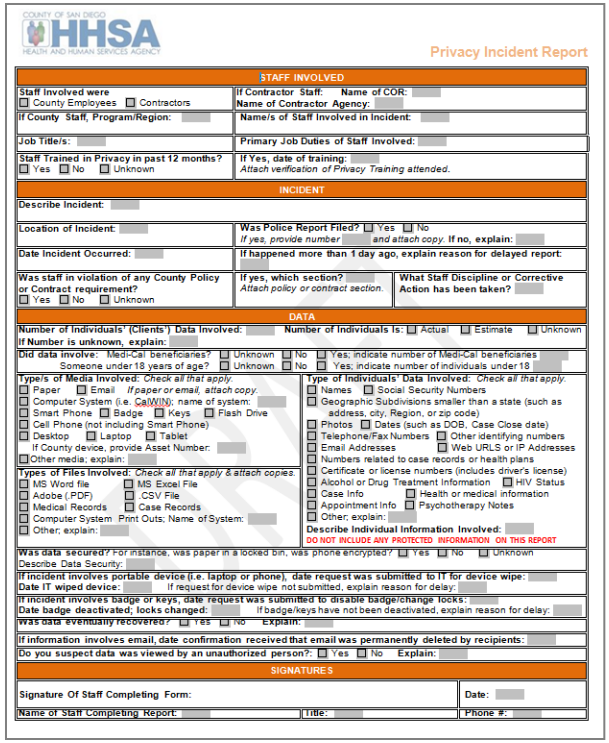
PRIVACY INCIDENT REPORTING

14.1.3.10 and 14.2.3.9

- Reportable Privacy Incidents include, *but are not limited to*:
  - Misplacing a client's chart
  - Giving Client A's paperwork to Client B (even if you immediately get it back)
  - Emailing a report with client information to the wrong person
  - Emailing Protected Information outside of your network in an unencrypted email (including replying to someone else's email)
  - Losing a laptop, phone, or tablet
  - Mailing client documents to the wrong
  - Throwing away client documents in the regular recycle bins
  - Copying client documents at a Kinkos
  - Car stolen with client chart inside (even if car and file later found)

PRIVACY INCIDENT REPORTING

- Immediately report to your COR and HHSA Agency Compliance Office
- Complete initial Privacy Incident Report (PIR) within one day; PIR is available online
- Send updated PIR within 3 days of initial report
- Completes final PIR within 5 days of initial report
- Also comply with SIR requirements



COUNTY OF SAN DIEGO HHSA HEALTH AND HUMAN SERVICES AGENCY

Privacy Incident Report

STAFF INVOLVED

Staff involved were ☐ County Employees ☐ Contractors
If Contractor Staff: Name of COR:
Name of Contractor Agency:
If County Staff, Program/Region:
Name/s of Staff Involved in Incident:
Job Title/s:
Primary Job Duties of Staff Involved:
Staff Trained in Privacy in past 12 months? ☐ Yes ☐ No ☐ Unknown
If Yes, date of training:
Attach verification of Privacy Training attended.

INCIDENT

Describe Incident:
Location of Incident:
Was Police Report Filed? ☐ Yes ☐ No
If yes, provide number and attach copy. If no, explain:
Date Incident Occurred:
If happened more than 1 day ago, explain reason for delayed report:
Was staff in violation of any County Policy or Contract requirement? ☐ Yes ☐ No ☐ Unknown
If yes, which section?
Attach policy or contract section.
What Staff Discipline or Corrective Action has been taken?

DATA

Number of Individuals* (Clients*) Data Involved: Number of Individuals is: ☐ Actual ☐ Estimate ☐ Unknown
If Number is unknown, explain:
Did data involve: Medi-Cal beneficiaries? ☐ Unknown ☐ No ☐ Yes; indicate number of Medi-Cal beneficiaries
Someone under 18 years of age? ☐ Unknown ☐ No ☐ Yes; indicate number of individuals under 18

Type/s of Media Involved: *Check all that apply.*
☐ Paper ☐ Email *If paper or email, attach copy.*
☐ Computer System (i.e. CalWIN); name of system:
☐ Smart Phone ☐ Badge ☐ Keys ☐ Flash Drive
☐ Cell Phone (not including Smart Phone)
☐ Desktop ☐ Laptop ☐ Tablet
If County device, provide Asset Number:
☐ Other media; explain:

Types of Files Involved: *Check all that apply & attach copies.*
☐ MS Word file ☐ MS Excel File
☐ Adobe (.PDF) ☐ .CSV File
☐ Medical Records ☐ Case Records
☐ Computer System Print Outs; Name of System:
☐ Other; explain:

Type of Individuals' Data Involved: *Check all that apply.*
☐ Names ☐ Social Security Numbers
☐ Geographic Subdivisions smaller than a state (such as address, city, Region, or zip code)
☐ Photos ☐ Dates (such as DOB, Case Close date)
☐ Telephone/Fax Numbers ☐ Other identifying numbers
☐ Email Addresses ☐ Web URLS or IP Addresses
☐ Numbers related to case records or health plans
☐ Certificate or license numbers (includes driver's license)
☐ Alcohol or Drug Treatment Information ☐ HIV Status
☐ Case Info ☐ Health or medical information
☐ Appointment Info ☐ Psychotherapy Notes
☐ Other; explain:
Describe Individual Information Involved:
DO NOT INCLUDE ANY PROTECTED INFORMATION ON THIS REPORT

Was data secured? For instance, was paper in a locked bin, was phone encrypted? ☐ Yes ☐ No ☐ Unknown
Describe Data Security:
If incident involves portable device (i.e. laptop or phone), date request was submitted to IT for device wipe:
Date IT wiped device: If request for device wipe not submitted, explain reason for delay:
If incident involves badge or keys, date request was submitted to disable badge/change locks:
Date badge deactivated; locks changed: If badge/keys have not been deactivated, explain reason for delay:
Was data eventually recovered? ☐ Yes ☐ No Explain:
If information involves email, date confirmation received that email was permanently deleted by recipients:
Do you suspect data was viewed by an unauthorized person?: ☐ Yes ☐ No Explain:

SIGNATURES

Signature Of Staff Completing Form: Date:
Name of Staff Completing Report: Title: Phone #:

QUESTIONS?

ANGIE DEVOSS, CHC, CHPC
Privacy Officer & Deputy Compliance Officer
County of San Diego
Health & Human Services Agency
Angie.DeVoss@sdcounty.ca.gov
619-338-2808
www.cosdcompliance.org