INFO PRIVACY & SECURITY

HHSA CONTRACTOR REQUIREMENTS & FAQ

Agency Compliance Office

County of San Diego - Health and Human Services

2021

ARTICLE 14 DISCLAIMER

These slides are intended to help HHSA contractors understand Article 14 requirements and address common questions from HHSA contractors related to Article 14

These slides are not a comprehensive summary of Article 14, nor does adherence to items discussed in these slides ensure an HHSA contractor's compliance with Article 14 or any other privacy and security rules. Likewise, an HHSA contractor may not need to comply with every item discussed herein. HHSA contractors are responsible for knowing which requirements apply to them and for ensuring their compliance with Article 14 requirements

These slides should not be considered legal advice

WHAT IS ARTICLE 14?

- Article 14 contains the Information Privacy and Security Provisions for HHSA contractors. These requirements can generally be found in the County contract template, section 14
- Article 14 requirements may vary based on the type of services you provide to HHSA and the funding streams that cover your contract
- More information on Article 14 can be found here: https://www.sandiegocounty.gov/content/sdc/hhsa/programs/sd/compliance_office/article_14.html

WHAT DOES ARTICLE 14 DO?

- Article 14 includes the County's Business Associate Agreement and may establish a contractor as the County's Business Associate
- Article 14 includes 42 CFR Part 2 and may establish a contractor as a Qualified Services Organization
- Article 14 includes requirements for all kinds of data, such as but not limited to: demographic data, financial data, social services data, and health care data
- Article 14 includes a bevy of State Agreements which may apply to your contract.
  - These State requirements apply broadly to many public health, behavioral health, eligibility operations, aging and independence services, and whole person care contracts
  - These State requirements are often more proscriptive than the privacy laws with which you may be familiar

ARTICLE 14 REQUIREMENTS

- Contractors are responsible for knowing which Article 14 requirements apply to them, including which State Agreements
- Contractors must ensure Article 14 requirements are passed down to all subcontractors, consultants, and other agents, as applicable
- Contractors must attest to their adherence with Article 14 requirements and complete monitoring tools related to these requirements
- Contractors must report all suspected security incidents and breaches (‘privacy incidents’) to HHSA and perform follow up as directed by HHSA

HOW DO I KNOW WHEN THE RULES APPLY?

- Article 14 contains definitions as to the types of information that must be protected. The definitions vary, based on which, if any, State Agreements apply to your contract, as well as which State and Federal laws apply to your data
- The following slides will cover some of the likely areas in which such protected information (PI) resides

EXAMPLES OF TECHNOLOGY COVERED BY ARTICLE 14

- Computer hard drives
- IT solutions, such as email, video chats, client electronic records, and calendaring software
- Memory inside a cell phone (voice mail, text messages, videos, pictures, call logs, contact lists, emails)
- Stand-alone cameras (not cell phones) issued to staff and/or cameras mounted to the wall in client areas
- Hard drives in fax machines, scanners, and copiers
- Local, network, and cloud servers
- It doesn't matter whether the PI is maintained/managed by you or a third-party vendor; Article 14 requirements still apply and you must ensure Article 14 requirements are included in your IT contracts

EXAMPLES OF OTHER MEDIA COVERED BY ARTICLE 14

- Paper, such as client charts, sign-in sheets, copies of photo IDs and insurance cards, client calendars, and internal reports for quality assurance
- Client areas – Interview rooms, lobbies, and reception areas – be mindful of PI that can anything be overheard or accessed
- Common areas, such as white boards in conference rooms or room assignment charts at residential programs
- Miscellaneous items - prescription medication bottles, medical equipment, other items given to clients and labeled with their information
- Any other medium that reasonably identifies the individual as belonging to your program and/or receiving health or social services

ADMINISTRATIVE REQUIREMENTS – COMMON TOPICS & FAQ

- Where can I get sample policies and procedures?
  - Internet search
  - County policies and procedures, found here: https://www.sandiegocounty.gov/content/sdc/hhsa/programs/sd/compliance_office/privacy_policies_procedures.html
  - Other contractors

- What is a security risk assessment or review (SRA)? Is this done by an IT company?
  - County Contractors can perform the SRA themselves or have a third-party conduct it.
  - An SRA template can be found at www.HealthIT.Gov

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

ADMINISTRATIVE REQUIREMENTS – COMMON TOPICS & FAQ

- What is the privacy and security training requirement?
  - Training for all workforce members – Workforce members include:
    - Positions paid by the contract, including those paid with indirect funds
    - Volunteers who support the contract
    - Those with access to County clients or County client data
  - Training both, at hire, and annually thereafter
  - Training certification, signed by staff; staff signature may be electronic

- What are Staff Confidentiality Statements?
  - Confidentiality Statements differ from training certifications
  - Confidentiality Statements are signed by workforce members prior to their access to PI
  - Confidentiality Statements must include, at a minimum, general use, security and privacy safeguards, unacceptable use, and enforcement policies

ADMINISTRATIVE REQUIREMENTS – COMMON TOPICS & FAQ

- Where can I find privacy and security training?
  - www.HealthIT.Gov has a variety of free training materials
  - The Agency Compliance Office can sometimes provide training to contractors
  - The Office of Civil Rights provides free training videos

- How do I know which subcontractors need Article 14?
  - Our Article 14 Decision Tree is available online

- How do I know whether my subcontractors are following Article 14?
  - What does your contract with them say? If it doesn't include Article 14, should it?
  - If it does include Article 14, how do you monitor your subcontractors?

- What 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.
  - Typically, Article 14 monitoring Tools are provided annually, although an Article 14 review may happen for any time, at the discretion of the County

TECHNICAL REQUIREMENTS – COMMON TOPICS & FAQ

- Is there a resource that can help contractors manage privacy and security?
  - www.HealthIT.Gov has a bevy of tools, templates, and guidance on various privacy and security topics, even those outside of health care
- What does “FIPS 140-2 certified algorithm” mean?
  - National Institute of Technology Standards
  - Your IT Staff or contractor should be able to address this for your specific IT assets
- What is a computer warning banner? Where do I get one?
  - 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
- How does Article 14 apply to bring your own device (BYOD) policies?
  - Once PI is accessed by/stored on/sent from these devices, they then must follow Article 14

TECHNICAL REQUIREMENTS – COMMON TOPICS & FAQ

- What kind of encryption is needed?
  - Two types of encryption are generally required, “at rest” and “in motion” encryption
    - “At rest” is encryption for data that lives on your devices, like data on your computer’s hard drive
    - “In motion” encryption is needed for data that is moving, such as an email you send to another agency
  - Encryption is not the same as password protection
  - There is no single type or brand of encryption, nor will every type of encryption work for every type of device

- Encrypted emails seem clunky. Any suggestions?
  - Contractors may consider setting up Transit Layer Services “encrypted tunnel” with the County so County and Contractor can email back and forth without having to manually encrypt and unencrypt individual emails
  - Contractors may explore allowing clients to opt out of encrypted email when the client makes such a request. HHSA’s policy and procedure for clients who request such alternate communications can be found here: https://www.sandiegocounty.gov/content/sdc/hhsa/programs/sd/compliance_office/privacy_policies_procedures.html

PHYSICAL REQUIREMENTS – COMMON TOPICS & FAQ

- What kind of locks are required for client's paperwork?
  - There is no specific type of lock required; Contractors must reasonably ensure the security of client paperwork as they do other PI
  - A general good rule is "two locks," but this is not a requirement
  - It is also not a requirement to use lock boxes when transporting client files

- Can I leave client files in the trunk of the car during home visits?
  - This varies based on the State Agreement that applies to your contract. Many State Agreements state that no PI may be left in the car, not even in a lockbox in the trunk

- What kind of security system is needed for my site?
  - Requirements vary based – check your State Agreement; a security guard or 24-hour monitored alarm system is not necessarily required
  - For locations that have staff onsite 24-hours a day, no additional staff may be needed

PHYSICAL REQUIREMENTS – COMMON TOPICS & FAQ

- Do all staff have to wear badges?
  - Badges are not necessarily required – this depends on your funding streams, scope of services, and your office setup

- What is meant by “escorting visitors”? Do we have to escort our own staff if they work at other sites? Our COR? Clients?
  - 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

HEALTH CARE REQUIREMENTS - COMMON TOPICS & FAQ

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

- What if my staff is going somewhere that does not allow them to bring anything in with them, like visiting a client in a locked facility?
  - 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

- If a client requests them, can staff send regular/unsecured texts to clients? Can they send unsecured/unencrypted emails?
  - HIPAA affords clients the right to request alternate communications. The County requires clients put these requests in writing (including via email). Our procedure and form can be found on our website: www.cosdcompliance.org
  - During COVID-19, clients may make these requests verbally or via text (see next slide)

ARTICLE 14 AND COVID-19

- Some requirements have been modified during COVID-19 to assist in the provision of remote services
- The Agency Compliance Office has released guidance related to the following:
  - Client Signatures and Verbal Consents during COVID-19
  - COVID-19 Telehealth
  - Text Messages for Client Communications
- The Agency Compliance Office also points to the following resources:
  - Office of Inspector General's Guidance on Waived or Reduced Share of Cost for Telecare
  - Office of Civil Rights' Guidance for Video Communication
- These resources can be found on the Agency Compliance Office website: https://www.sandiegocounty.gov/content/sdc/hhsa/programs/sd/compliance_office/COVID-19-resources.html

PRIVACY INCIDENT REPORTING REQUIREMENTS

- Contractor shall email their COR and HHSA Privacy Officer immediately upon the discovery of a suspected security incident that involves data provided to County by the Social Security Administration, as per the State Agreements
- Contractor shall email COR and HHSA Privacy Officer immediately of breaches and suspected privacy incidents involving 500 or more individuals
- Contractor shall additionally submit an online County "Privacy Incident Report" through the online portal at www.cosdcompliance.org within one (1) business day for all breaches and suspected security incidents
- Detailed definitions of suspected security incidents, breaches, and privacy incidents can be found in Article 14 and its referenced agreements

PRIVACY INCIDENT REPORTING REQUIREMENTS

- Reportable Privacy Incidents include, *but are not limited to*:
  - Cyber threats and ransomware attacks on systems/networks that contain client information
  - Misplacing a client's chart or file
  - 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
  - Losing a laptop, phone, or tablet that contains or can access client information
  - Mailing client documents to the wrong address or client
  - Car stolen with client information inside
    - Even if car and information are later found
    - Even if information was in a lock box
  - Staff accessing client records without a business reason

AGENCY COMPLIANCE OFFICE RESOURCES

The Agency Compliance Office has several resources available to help contractors manage Article 14 requirements, including:

- Privacy and Security Walk-Throughs
- Trainings for Privacy and Security Officers on Article 14 requirements
- Trainings for line staff on privacy rules
- Privacy Policies, Procedures, & Forms

MORE QUESTIONS? ASK US!

Christy Carlson

Group Program Manager

Christy.Carlson@sdcounty.ca.gov

619-338-2807

Angie DeVoss

Privacy and Deputy Compliance Officer

Angie.DeVoss@sdcounty.ca.gov

619-338-2808