Provider FAQ

Information Privacy and Data Security Provisions (Article 14)

- **What are the Information Privacy and Security Provisions (Article 14)?**

  Article 14 outlines requirements related to privacy, confidentiality and data security of Protected Information. Article 14 contains various regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) and 42 CFR Part 2. It serves as HHSA's Business Associate Agreement and contains additional privacy and security requirements from the State of California (State Agreements). It also includes a process for providers to report breaches and suspected security incidents involving Protected Information.

  Article 14 may also be used to pass on a general privacy statement that references State or federal laws that are specific to the type of funding, population served, and/or manner in which information is stored and shared in a specific contract.

- **Where can providers find Article 14 requirements?**

  Typically, Article 14 requirements are found in the contract template. The latest version of Article 14, as well as links to the included State Agreements, can be found here. Additional provider resources can be found here.

- **Which parts of Article 14 apply to my contract?**

  Whether regulations, such as HIPAA or 42 CFR Part 2, apply to your contract is best determined by the provider's legal counsel. Which, if any, State agreement applies is typically contingent on funding streams and data access. COR teams can assist providers with making that determination. The breach and suspected security incident reporting process applies to all contracts that contain Article 14.

- **Which information falls under the Article 14 provisions?**

  Article 14 contains definitions of 'County Protected Health Information' and 'County Personal Information/ Personally Identifiable Information'. Providers should pay attention to these definitions when making decisions about Article 14 applicability.

- **Which staff fall under Article 14 provisions?**

  Any workforce member, whether paid or unpaid, employed or subcontracted, who has access to Protected Information needs to follow Article 14 requirements. This includes, but is not limited to: client facing positions, support positions, and those with access to any network or device that contains or provides Protected Information.

Information Privacy and Security Provisions (Article 14)

- **How do I handle Article 14 provisions for subcontractors or consultants?**

  Providers must include all applicable Article 14 requirements in their subcontractor and consultant agreements. Which Article 14 provisions the provider chooses to manage for subcontractors or consultants versus which requirements the provider chooses to have the subcontractor or consultant manage is up to the provider; however, this should be formally delineated.

- **What is a Security Risk Assessment or System Security Review? How does it get completed? How should it be documented?**

  A Security Risk Assessment (SRA) is a term employed by HIPAA, whereas a System Security Review (SSR) is a term outlined in the State Agreements. Many agencies ensure both the SRA requirements and the SSR requirements are completed within a single risk assessment. Some agencies perform the assessment annually, while others perform it in pieces on a rolling basis. Some agencies conduct it in-house; others hire a third party.

  While HHSA does not have a third-party company to recommend, the Office of the National Coordinator for Health Information Technology provides this free tool.

  Regardless of how a provider chooses to conduct the assessment, documentation of the assessment is important and generally should include: areas assessed, by whom, and the date; risk assessed, by whom, and the date; mitigations planned/performed, by whom, and the date. The review of the assessment, any assessment follow-up, and the assessment process overall are generally documented as well.

- **What if I have questions about sharing HHSA clients' Protected Information?**

  Many questions related to sharing information will need to be addressed by the provider's privacy professionals and/or legal counsel. BAC's privacy resources, including the HHSA Release of Information form, and policies and procedures on sharing information, can be found here.

- **Can you explain the Privacy Incident Report (PIR) process?**

  The PIR process includes the steps by which providers report a breach or suspected security incident to HHSA. For most privacy incidents, providers need to submit a PIR within 1 business day of discovery, using the HHSA online portal, found here.

  Significant privacy incidents, such as those involving Social Security Administration data, or those involving more than 500 individuals, require quicker reporting. Providers may also submit follow-up PIRs, breach risk analysis, mitigations, and notifications, which are outlined in Article 14.

- **Does HHSA offer any training on or assistance with Article 14?**

  Yes, the Business Assurance and Compliance (BAC) provides tailored training for provider staff related to privacy and security requirements. BAC can also meet with provider privacy and security officials to talk through areas of confusion and/or perform privacy and security walk-throughs to help providers manage Article 14 requirements and privacy and data security best practices.

Information Privacy and Security Provisions (Article 14)

- **How does HHSA typically monitor providers' Article 14 compliance?**

  Article 14 monitoring differs across contracts. Typically, COR teams will ask providers to complete an Article 14 monitoring tool annually. The components of the tool will vary each year. HHSA may also perform additional Article 14 review following a Privacy Incident Report or on an ad-hoc basis.

- **What is the best way to provide Protected Information to a COR?**

  Article 14 requires that Protected Information be secured at all times. HHSA generally uses encrypted email to send Protected Information, although other secure methods of transmission, like faxing, are acceptable as well. HHSA recommends that providers set up a secure Transit Layer Security connection, so encrypted emails can be sent back and forth seamlessly by provider and HHSA staff without having to manage manual encryption processes.

Don't see your question answered above? Have additional questions? Your COR team is your primary resource for any questions related to your HHSA contract. For questions related to this FAQ, please contact HHSA Business Assurance and Compliance (BAC) by email at Compliance.HHSA@SDCounty.ca.gov or by phone (619) 237-8571.