Privacy & Security Requirement Sources

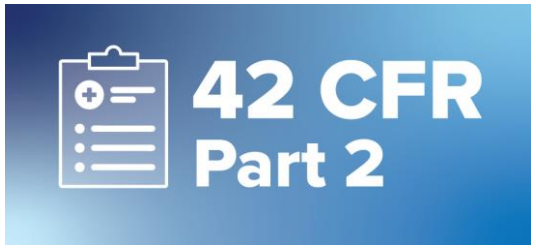
- **Federal & State Laws & Regulations**
  - Health Information Portability & Accountability Act (HIPAA) (All health)
  - 42 CFR Part 2 (SUD)
  - California Welfare & Institutions Code 5328 (Mental Health)
  - **Contract Provisions**
  - Exhibit A-1: Standard Requirements, VI. Client Records, Data, Privacy, and Security Requirements
  - Exhibit E: Business Associate Agreement
  - Exhibit A-3: Qualified Service Organization Agreement
- **ACBH Policies & Procedures**
  - #350-3-1: Privacy, Security, and Confidentiality Statement of Client Services, Records, and Information
  - #1704-1-1: Privacy & Security Incident Reporting Policy

Key Privacy Requirements

- Protect all individually identifiable health information
- **Minimum necessary rule:** limit the use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose
  - Exceptions: treatment, disclosures to client, authorization (Release of Information)
- When in doubt, obtain a valid **Release of Information** to disclose Protected Health Information (PHI)
- Train all workforce and require Confidentiality Attestation for all staff at onboarding and annually

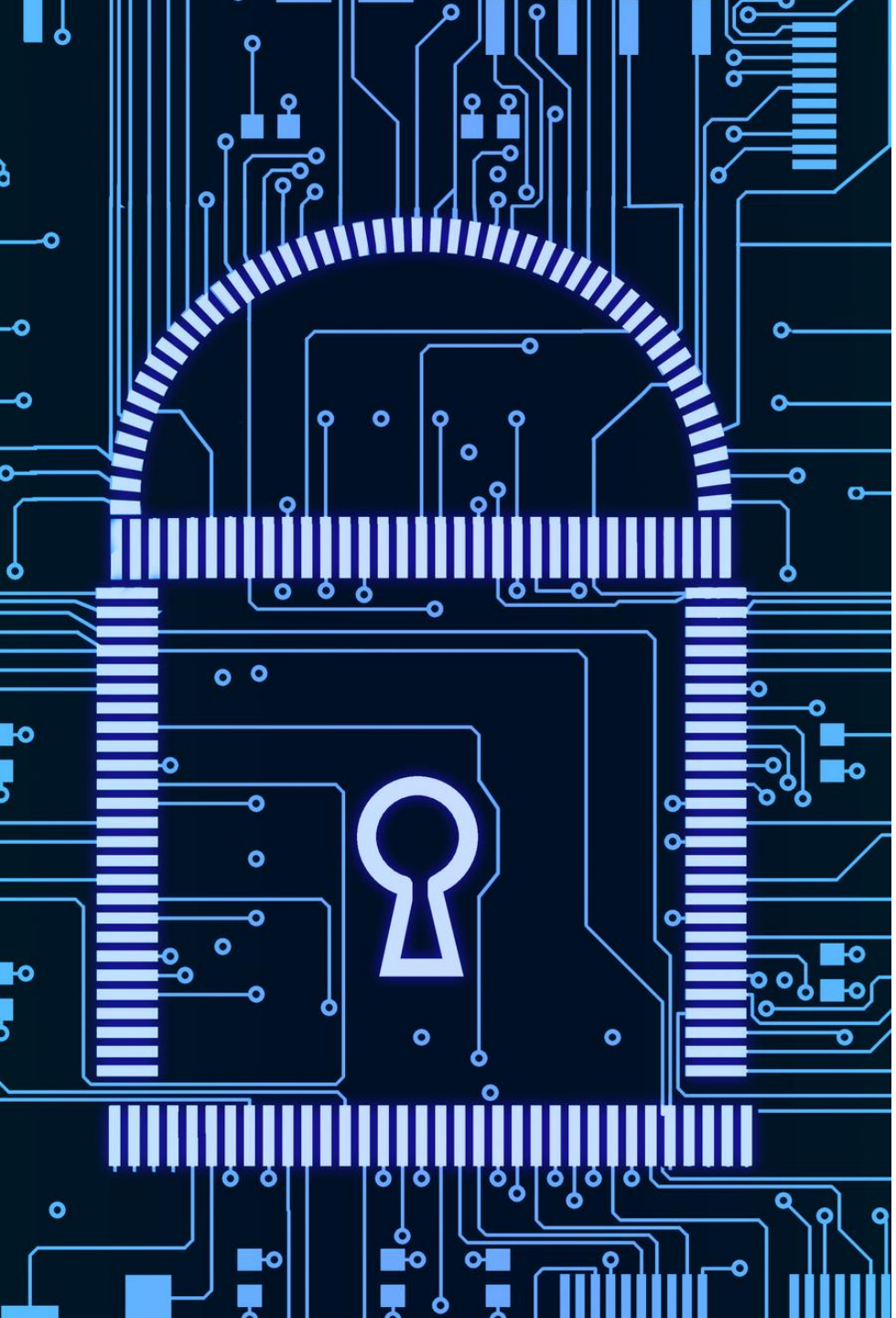
Key Privacy Requirements (Ctd.)

- **Report ALL privacy/security INCIDENTS, not just breaches, to Privacy Officer**
- **Mitigate** any harmful effect as a result of a breach
- Require any **agent or subcontractor** to follow Privacy Rule, Security Rule, and contractual requirements through written contracts through Business Associate Agreement/Qualified Service Organization Agreement
- Upon request of client or client representative:
  - Make PHI available in designated record set
  - Make accounting of disclosures available
  - Allow amendments to designated record set
- If contract is terminated, PHI must be returned or destroyed



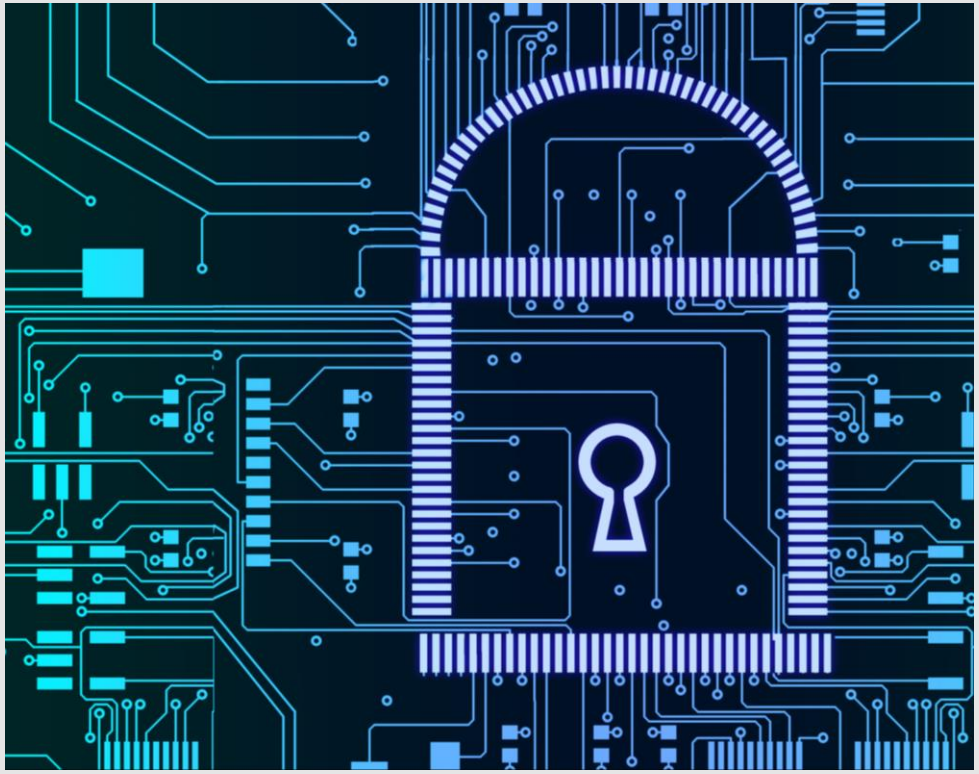
Special Requirements – Substance Use Disorder Information

- 42 CFR Part 2 is generally more restrictive regarding use and disclosure and re-disclosure of SUD information from an SUD provider
- Releases of Information (ROIs) are almost always required to disclose or re-disclose SUD information
  - Exceptions: medical emergency to medical provider, audit & evaluation, research
  - CARES Act will modify 42 CFR Part 2, to be revised TBD 2022
  - Note: ACBH will be issuing new SUD ROIs soon



Key Security Requirements

- Follow all Security Rules & HIPAA Security Regulations
  - Implement administrative, physical, and technical safeguards
  - Perform risk analysis and management
  - Must have Security Officer
  - Must manage information access to follow minimum necessary requirement (i.e., role-based access)
- Electronic Health Records must have warning banner concerning PHI
- Emails with PHI must be sent in a secure, encrypted manner
- Password management policies should include requiring passwords be changed every 90 days
- Notify ACBH IS immediately if any staff with access to PHI or PII through ACBH's applications (e.g., Clinician's Gateway, InSyst, Yellowfin) depart from the organization or change functions and no longer need this access so that ACBH can terminate/amend access.



Privacy Incident Steps

- Notify ACBH Privacy Officer **within 24 hours** of any **suspected** or actual breach of security, intrusion, and/or use/disclosure of PHI in violation of federal/state laws/regulations
- Submit Privacy Incident Report Form to ACBH currently via email breachnotification@acgov.org; *will change to online format soon*
- Investigate breach and take prompt corrective action to address deficiencies as required by laws/regulations
- Provide written report of investigation to ACBH Privacy Officer, including identification of each individual whose PHI has been breached within 15 working days of discovery of breach
- Notify individuals of breach, pending directions from ACBH

ACBH Privacy & Security Team

- ACBH Privacy Officer: Sophia Lai, Sophia.Lai@acgov.org
- ACBH Security Officer: Priya Bala, Priya.Bala@acgov.org
- ACBH Privacy Administrative Support: TBD
- HCSA Chief Compliance & Privacy Officer: Ravi Mehta, Ravi.Mehta@acgov.org