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 F: 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
  - Primary exceptions: treatment, disclosures to client, pursuant to authorization (Release of Information)
- When in doubt, obtain a valid **Release of Information** to disclose Protected Health Information (PHI)
- Train all workforce and require Oath of Confidentiality for all staff at onboarding and annually

Key Privacy Requirements (Ctd.)

- **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
- 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 are almost always required to disclose or re-disclose SUD information
  - Exceptions: medical emergency, audit & evaluation, research
  - CARES Act will modify 42 CFR Part 2, to be revised March 2021

Key Security Requirements

- Must follow all Security Rule & HIPAA Security Regulations
  - Implement administrative, physical, and technical safeguards
  - Must 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

Key Security Requirements – Cont.

Confidentiality, Integrity and Availability (CIA) are the guiding principles for HIPAA security. Here is a checklist guide for software compliance:

- User Authorization
- Access Control
- Authorization monitoring
- Data Backup
- Emergency Mode
- Auto logoff
- Data encryption and decryption (at rest and transit)
- Auditing

Privacy Incident Steps

- Notify ACBH Privacy Team **within 24 hours** of any suspected or actual breach of security, intrusion, HIPAA, and/or use/disclosure of PHI in violation of federal/state laws/regulations
- Submit Privacy Incident Reporting Form to ACBH via email breachnotification@acgov.org or by phone at 1-844-729-7055
- Investigate breach and take prompt corrective action to address deficiencies and 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, following directions of ACBH

ACBH Privacy & Security Team

- ACBH Privacy Officer: Sophia Lai, Sophia.Lai@acgov.org
- ACBH Security Officer: Jennifer Moore, Jennifer.Moore@acgov.org
- ACBH Privacy Administrative Support: Tiffany Lynch, Tiffany.Lynch@acgov.org
- HCSA Chief Compliance & Privacy Officer: Ravi Mehta, Ravi.Mehta@acgov.org