Legal and Compliance Considerations for Connecting Diverse Entities

Community Information Exchange SUMMIT

- Shelley Brown, San Diego Health Connect
- Jennifer Behrens, KUMA
- Ford Winslow, ICE Security

LEGAL CONSIDERATIONS FOR CONNECTING DIVERSE TYPES OF ENTITIES -

A PRACTICAL APPROACH FOR ADDRESSING PRIVACY AND SECURITY REQUIREMENTS FOR DATA EXCHANGES

PRESENTER: MICHELLE (SHELLEY) BROWN, ESQ.

PRIVACY AND REGULATORY AFFAIRS ADVISOR

THREEFOLD APPROACH

- DOCUMENTATION
- PROCESS
- CLIENT/PATIENT COMMUNICATION

ADDRESS PRIVACY AND SECURITY COMPLIANCE IN THE TRUSTED FRAMEWORK DOCUMENTATION

DATA USE AGREEMENT

BUSINESS ASSOCIATE AGREEMENT

POLICIES AND PROCEDURES

NOTICE OF PRIVACY PRACTICES

REINFORCE COMPLIANCE DURING IMPLEMENTATION AND THROUGH ONGOING MONITORING OF PARTICIPANT ACCESS TO DATA

ONBOARDING

TRAINING

USER ACCESS

AUDIT AND ALERTS

ENSURE THE DATA EXCHANGE STORES AND EXCHANGES DATA IN COMPLIANCE WITH REGS

Privacy and Security Requirements begin with an evaluation of the Data SOURCE.

- Client Self Reported Data: Manage Privacy Expectations
- Personally Identifiable Information: Data collected or created by businesses providing Goods and Social Services.
- Protected Health Information: Data created or in the possession of a Regulated Entity such as a HIPAA Covered Entity, or Program under 42 CFR Part 2 (Substance Use Disorder)

MANAGE CLIENT'S PRIVACY EXPECTATIONS

Notice of Privacy Practices: Provide information about how data will be used, stored and exchanged –

Client Consent/Authorization: Document the Client's understanding and Consent to share Client Information. If Data includes health information - obtain the Client's Authorization.

Use Client Data to provide services for or for the benefit of the Client. (Avoid the Facebook Fallout)