

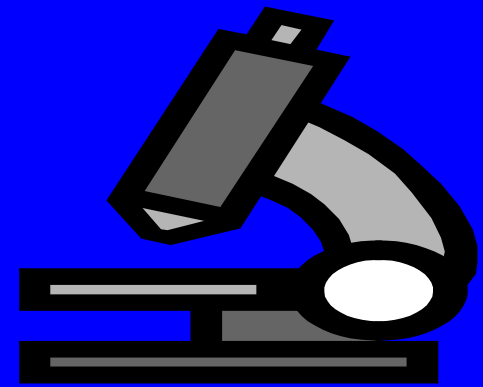
Davis Wright Tremaine LLP 

HIT Legal Issues: HIPAA Implications to a Regional Health Information Organization

Becky Williams, R.N., J.D.
Partner, Co-Chair, HIT/HIPAA Practice Group
Davis Wright Tremaine LLP
206-628-7769
beckywilliams@dwt.com

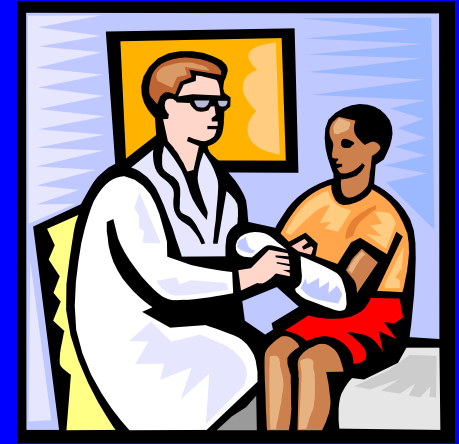
HIPAA Analysis: Starting Point

- Identify those with access
 - Determine covered entity status
 - Determine other status (e.g., business associate)
- Examine the Flow of PHI within the RHIO
 - Covered Provider ↔ Covered Provider
 - Covered Provider ↔ Non-Covered Provider
 - Covered Provider ↔ Plan
 - Covered Entity ↔ Non-Covered Third Party
- Purposes of the PHI Flow



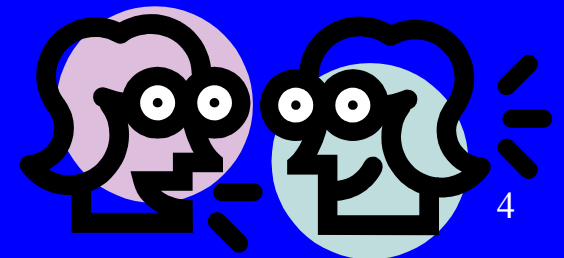
Ways to Disclose: TPO

- **May disclose PHI for own**
 - **Treatment**
 - **Payment**
 - **Operations**
- **May disclose PHI for treatment activities of a health care provider (not necessarily a covered provider)**
- **May disclose PHI to provider or covered entity for payment purposes**
- **May disclose PHI to covered entity**
 - **For limited operations (e.g., QA, peer review, compliance)**
 - **If both have/had relationship with patient**
 - **If disclosure relates to relationship**



Ways to Disclose: OHCA

- Medical Staff OHCA
- Community OHCA: organized system of health
 - More than one covered entity
 - Hold themselves out to the public as a joint arrangement
 - Participate in joint activities that include UR, QA or sharing of financial risk
- May disclose PHI to another covered entity in OHCA for OHCA health care operations





Ways to Disclose: Business Associate

- Business Associate provides services on behalf of a covered entity involving PHI
 - Examples: management, administration, data aggregation
- Need BAC
- RHIO/ASP/ISP
 - May or may not be covered entity
 - May be a business associate (especially in a hub and spoke arrangement)



Ways to Disclose: Patient Authorization

- May not be necessary for most disclosures
 - Depends on participants
 - When in doubt, go with an authorization
- State law may present greatest challenges
 - May be more stringent on disclosures
 - May present problems with authorization
 - Requirements likely to vary with type of info (mental health, AIDS/HIV/STD, developmental disabilities, substance abuse)
- Beware of federal substance abuse requirements
- May want to seek patient permission/acknowledgement
 - Puts patients on notice; helps to avoid surprises
 - Opportunity to request additional privacy protections



Ways to Disclose: Non-PHI

■ De-identified data

- May be aggregated/shared
- Is it truly de-identified?

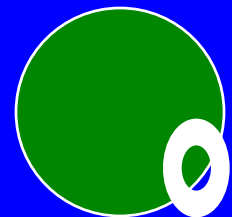
■ Limited data sets

- For public health, research or operations
- Need data use agreement



Minimum Necessary

- May use, disclose or request only the *minimum necessary* information for the intended purpose
- RHIO members may rely on other members' representation if
 - All are covered entities and
 - Reliance “is reasonable under the circumstances”
- No minimum necessary for
 - Treatment
 - Authorization



Individual Rights

■ General Issues

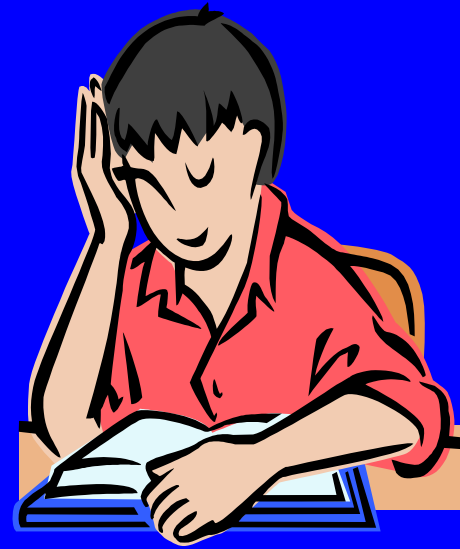
- Need to determine responsibilities
- Centralized v. de-centralized

■ Access

- If de-centralized, different providers may follow different rules
- Want to put participants on notice

■ Amendment

- Provider to make determination
- Process for making amendments system-wide
- Need to preserve pre-amendment PHI
- Need to track timing of amendments
- Need to link to statement of disagreement/rebuttal





Individual Rights

- **Accounting of disclosure**
 - Most RHIO disclosures not subject to accounting
 - Who tracks?
- **Request additional privacy protection**
 - Covered entity has right to refuse
 - Accepted request → Bound
 - Practical implication: Is RHIO bound?
 - Be aware of system limitations
- **Notice of privacy practices**
 - Want all participants to include description of community-wide system
 - Each party is responsible for contents/distribution of NPP
 - Joint NPPs need to be tracked



Administrative Responsibilities

■ Training

- Centralize v. decentralized

■ Sanctions

- Each member must have and use sanctions
- Collaborative – wide sanctions

■ Policies

- Individual policies and procedures
- Rules of the road



Security Standards

- Standards are scalable based on sophistication and resources of covered entity
- Security is only as good as the weakest link
- Minimum standards may be required (e.g., through user/license agreement)
- Systems protections for appropriate access
 - Identify relationship with patient
 - Break the glass
- Audit/sanctions

