Privacy and Security Challenges in Integrated Care

Presented by: Tim Timmons
CCEP, CHPC, CHP, CHSS

Personal Introduction

- Current responsibilities
  - Compliance, privacy and information security officer for an organization that used to be a managed care organization delivering mental health services to Medicaid beneficiaries in 16 rural counties in Oregon
  - GOBHI is now a partner/stakeholder in three coordinated care organizations in Oregon covering 17 rural counties

The Challenge

- In Oregon, we have both Federal and State mandates to promote and utilize health information technology to accomplish the Triple Aim
  - Better health
  - Better care
  - Lower per capita cost
- Health care providers need to be able to exchange health information electronically in order to achieve the Triple Aim
Oregon Mandate

Senate Bill 1580

- SECTION 16. (1) Notwithstanding ORS 179.505, a health care provider that is a participant in a coordinated care organization, as defined in ORS 414.025, shall disclose protected health information:
  (a) To other health care providers participating in the coordinated care organization for treatment purposes, and to the coordinated care organization for health care operations and payment purposes, as permitted by ORS 192.558…

Oregon Mandate

- Are any of the provisions in ORS 179.505 that are more stringent than HIPAA still in force?

- If ORS 179.505 has been removed as a barrier to PHI disclosure, what about other Oregon privacy statutes that affect health care providers and payers?
  - OAR 407.014.0000 and 0020 (See Handout)

Oregon Mandate

ORS 430.399(5)

- (1) Any person who is intoxicated or under the influence of controlled substances in a public place may be taken or sent home or to a treatment facility by the police….
Oregon Mandate

ORS 430.399(5)

- The records of a patient at a treatment facility may not be revealed to any person other than the director and staff of the treatment facility without the consent of the patient. A patient’s request that no disclosure be made of admission to a treatment facility shall be honored unless the patient is incapacitated or disclosure of admission is required by ORS 430.397.

Federal Law

42 U.S. Code § 290dd–2(a) - Confidentiality of Records

- Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall...be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section.

Privacy Challenges

Figuring out who you can share PHI with if you don’t have the patient’s consent – not all stakeholders are HIPAA covered entities. Ideally, hot spotting should include, for example:

- School system personnel
- Child welfare agencies – child abuse investigations
- Senior services agencies – elder abuse investigations
- Developmental disabilities agencies
- County commissioners
Privacy Issues

Sharing PHI protected under 42 CFR Part 2

- No TPO exception to authorization requirement
- Qualified service organizations may exchange PHI directly with the A&D provider, but not with anyone else
- HIQs may be QSOs

Privacy Issues

Sharing PHI protected under 42 CFR Part 2

- The minimum necessary PHI may be shared with the organization that has administrative control over the A&D program
- Information that identifies the individual as being in treatment for substance abuse may not be disclosed

Privacy Solutions

- If OHA requires that certain client information be shared with the Authority, and Part 2 restricts the disclosure of that information without the clients authorization, it would appear that all A&D clients would need to authorize such disclosures
- What recourse does a Part 2 program have if the client refuses to authorize the disclosure requested?
Security Challenges

- Oregon has a statutory mandate to facilitate electronic health information exchange in a way that supports exchange of PHI among participating providers to transform from a volume-based to a value-based delivery system.

The Good News

- ONC Privacy & Security Program Information Notice (PIN):
  “Where HIE entities serve solely as information conduits for directed exchange of individually identifiable health information (IIHI) and do not access IIHI or use IIHI beyond what is required to encrypt and route it, patient choice is not required beyond existing law.”

The Bad News

- But, the ONC goes on to say “Where HIE entities store, assemble, or aggregate IIHI beyond what is required for an initial directed transaction, HIE entities should ensure individuals have meaningful choice regarding whether their IIHI may be exchanged through the HIE entity. This type of exchange will likely occur in a query/response model or where information is aggregated for analytics or reporting purposes.”
The Bad News

Patients opting out:

- Force providers to either go back to faxing or mailing records, or to use directed exchange to share PHI for treatment purposes, which obviously decreases operational efficiency and realistically precludes multiple exchanges with multiple integrated providers
- Make is practically impossible to collect the analytics required for reporting outcomes measures and other performance metrics

Financial Challenges

- Behavioral health providers can receive incentive payments for the adoption of health information technology only if they have a psychiatrist or nurse practitioner on staff
- The Behavioral Health Information Technology Act (H.R. 2957) would add community mental health centers, psychiatric hospitals, mental health treatment facilities and substance abuse treatment centers to the list of organizations eligible for federal incentive payments

HIE Challenges

- Lack of broadband capabilities in rural/remote areas
- Lack of funds to invest
- Lack of expertise in smaller provider organizations. Some smaller providers have no IT personnel on staff
- EHR systems who don’t communicate with each other
- Developing a business model that's sustainable, that meets the data needs of all healthcare providers, and keeps all the competing participants onboard is a challenge
HIE Challenges

• Beyond the actual technology issues involved with keeping patient data exchange secure are deeper worries related to governance – HIEs require competing healthcare entities to trust one another

• If individuals and other participants in a network lack trust in the exchange of electronic information due to perceived or actual risks to their individually identifiable health information, or the accuracy and completeness of such information, they may be unwilling to consent to the disclosure of electronic PHI

Consequences of a Lack of Trust

A lack of willingness to consent to the disclosure of electronic PHI:

• Could have life-threatening consequences
• Would compromise the efficiency of the delivery system
• Would make it much more difficult to capture the analytics necessary to report on outcomes, cost efficiency of treatment, provider performance, quality of care and improvements in the health of the population

HIE Challenges

• Sustainability is a function of the number of partners participating in the HIE and commitment by large organizations that carry the regional effort

• If an HIE loses a big player over issues involving trust or secure data access and exchange, sustainability will be compromised
The Ultimate Challenge

- The ultimate problem, however, is that you’re dependent upon the people sharing the health information to comply with Federal and State laws and your privacy and security policies and procedures

- That highlights the importance of a culture of compliance which is supported by ongoing education, auditing and monitoring, and ensuring there are consequences for non-compliance

The Ultimate Challenge

- The other challenge is to earn the patient’s trust that his/her PHI will be protected and not made accessible to someone who shouldn’t or doesn’t need to see it, particularly if it’s in electronic form

- If the NSA can’t protect its information, how much confidence can I have in my health care provider to safeguard my PHI?

- Is privacy dead in healthcare?

QUESTIONS?

Tim Timmons
Corporate Integrity Officer
Greater Oregon Better Health Initiative

tim.timmons@gobhi.net
Phone: 503-931-9867