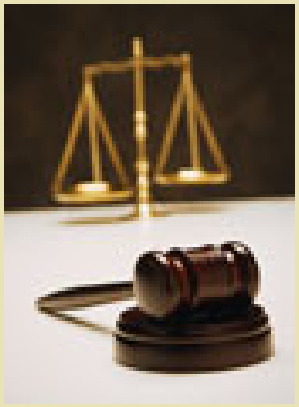
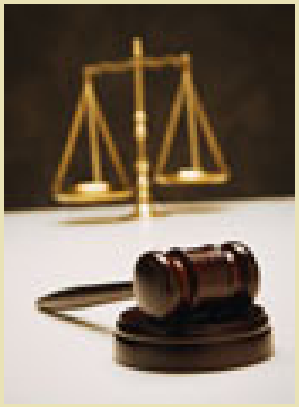


Privacy and Security Challenges in Integrated Care

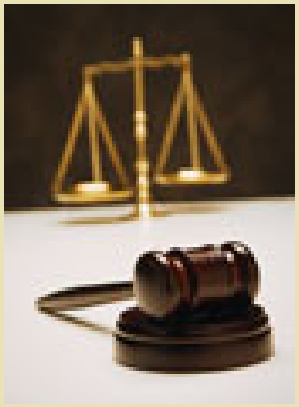
Presented by: H. M. (Tim) Timmons, Jr.

CCEP, CHPC, CHP, CHSS



Personal Introduction

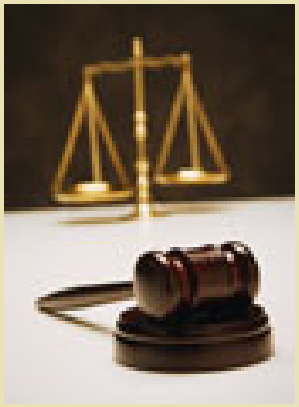
- Current responsibilities
- Compliance, privacy and information security officer for an organization that used to be a managed care organization delivering mental health services to Medicaid beneficiaries in 16 rural counties in Oregon
- GOBHI is now a partner in three coordinated care organizations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



Why Do We Need Integrated Care?

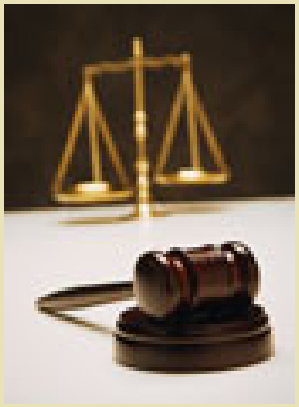
The existence of silos in the health care delivery system results in:

- Operational inefficiencies,
- Unnecessary costs,
- Increased patient dissatisfaction
- The potential for compromised outcomes and quality
- More fundamentally, it does not support an integrated effort to improve the health of the population by addressing the conditions that drive both the need for and the cost of medical care.



Why Do We Need HIE?

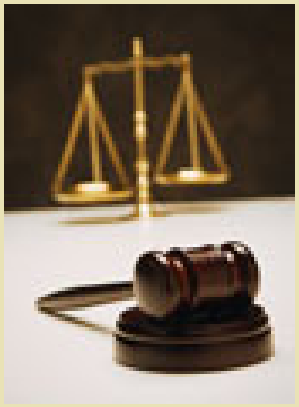
- In order to improve the health of the population, increase the quality, reliability and availability of health care services and to lower or contain the cost of care so it is affordable (the Triple Aim), information must flow synergistically across all domains, through all business process and among all authorized users



Why Do We Need HIE?

In order to achieve these objectives, the use of technology to exchange health information becomes increasingly important in order to:

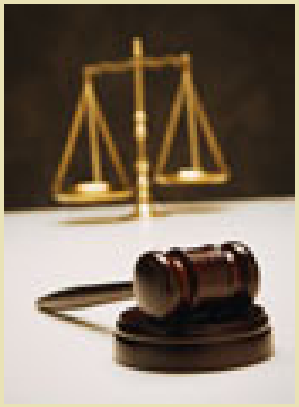
- Reduce medical errors
- Reduce health care costs
- Reduce the redundancy of services
- Improve health care quality and outcomes
- Enable consumers to better communicate with their providers and manage their personal health, resulting in fewer office visits and better disease management



The Challenge

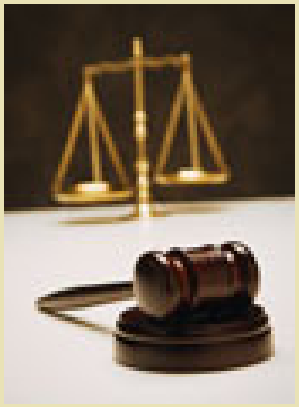
- In Oregon, we have both Federal and State mandates to promote and utilize health information technology to accomplish the Triple Aim

- Health care providers need to be able to exchange health information electronically in order to achieve the Triple Aim



The Challenge

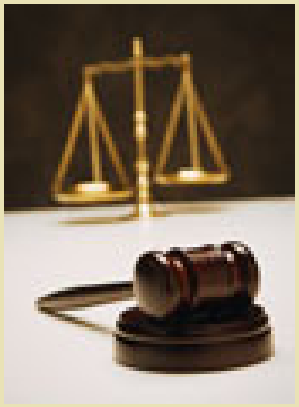
- However, if individuals and other participants in a network lack trust in the exchange of electronic information due to perceived or actual risks to their individually identifiable health information, or the accuracy and completeness of such information, they may be unwilling to consent to the disclosure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



The Challenge

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

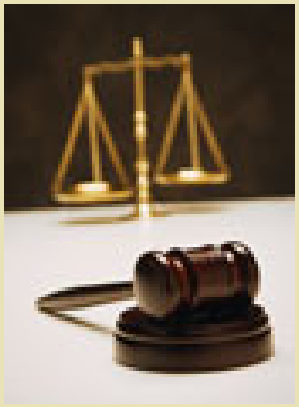
- Could have life-threatening consequences
- Would compromise the efficiency of the delivery system
- Would make it much more difficult to capture the analytics necessary to report on outcomes, cost efficiency of treatment, provider performance, quality of care and improvements in the health of the population



Privacy Issues

Figuring out who you can share PHI with if you don't have the patient's consent - not all stakeholders are HIPAA covered entities.

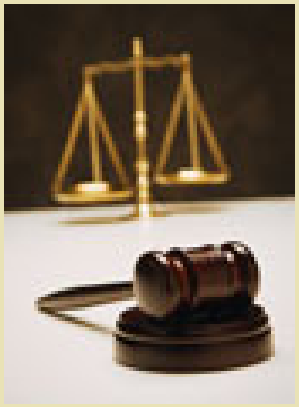
- Public health agencies
- Schools
- Child welfare agencies – child abuse investigations
- Senior services agencies – elder abuse investigations
- Developmental disabilities agencies
- County commissioners



Privacy Issues

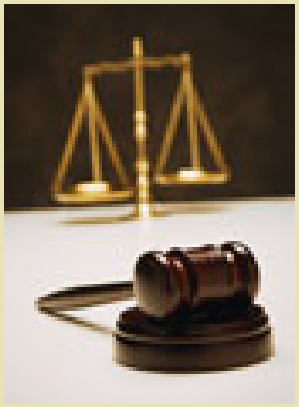
- Sharing PHI protected under 42 CFR Part 2 – Substance abuse treatment programs

- Ensuring that stakeholders that aren't covered entities don't receive electronic PHI without patient consent, and that only the minimum necessary PHI is sent when required



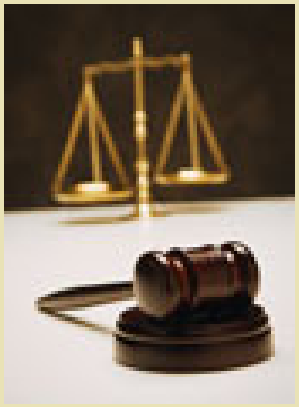
Privacy Solutions

- Organized Health Care Arrangement – For providers that do not deal with specially protected PHI
- Qualified Service Organization Agreements – For substance abuse treatment providers



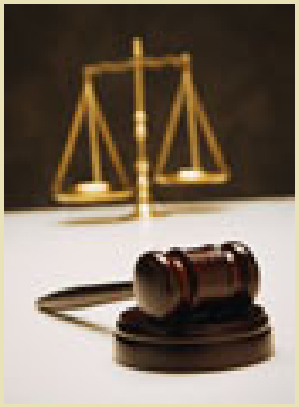
Security Challenges

- 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



Security Challenges

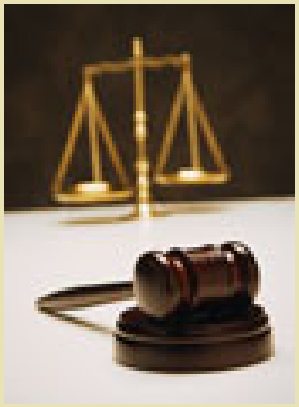
- In order to accomplish that transformation, coordinated care organizations (CCOs) should initially identify current capacity and then develop and implement a plan for improvement (including benchmarks and evaluation points)



Security Challenges

The plan for improvement should include benchmarks and evaluation points in the follow areas:

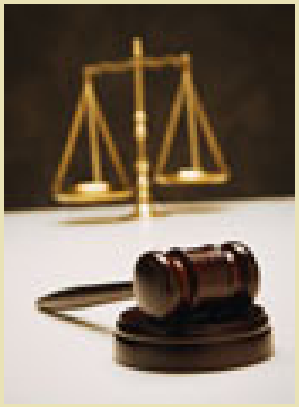
- Analytics used in reporting outcomes measures to the CCO's provider network to assess indicators such as provider performance, effectiveness and cost-efficiency of treatment
- Quality reporting to support quality improvement within the CCO's provider panel and to report the data on quality of care necessary for the Oregon Health Authority to monitor the CCO's performance



Security Challenges

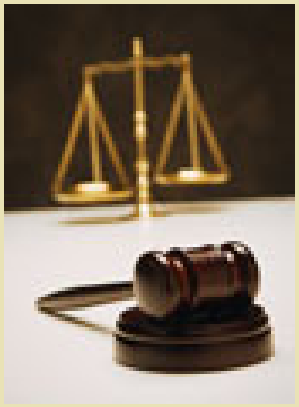
- ONC Privacy & Security Program Information Notice (PIN):

"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."



Security Challenges

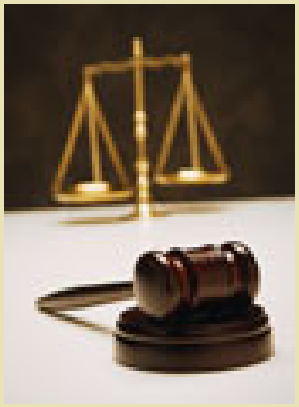
- But, the ONC goes on to say “Where HIE entities store, assemble, or aggregate IIHI beyond what is required for an initial directed transaction, HIE entities should ensure individuals have meaningful choice regarding whether their IIHI may be exchanged through the HIE entity. This type of exchange will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



Security Challenges

Patients opting out:

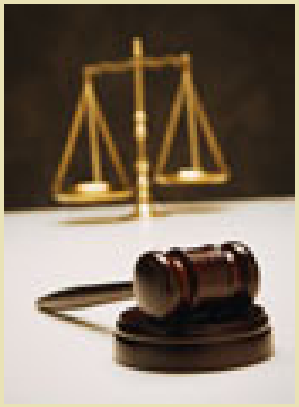
- Force providers to either go back to faxing or mailing records, or to use directed exchange to share PHI for treatment purposes, which obviously decreases operational efficiency and realistically precludes multiple exchanges with multiple integrated providers
- Make is practically impossible to collect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



Security Challenges

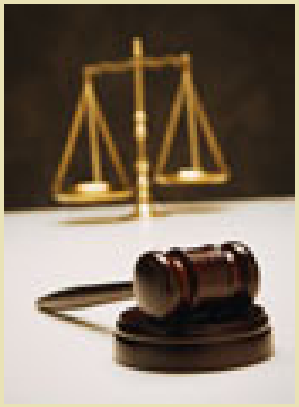
- Behavioral health *providers* can receive incentive payments for the adoption of health information technology only if they have a psychiatrist or nurse practitioner on staff

- The Behavioral Health Information Technology Act (H.R. 6043), much like it counterpart in the Senate (S.539), will 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



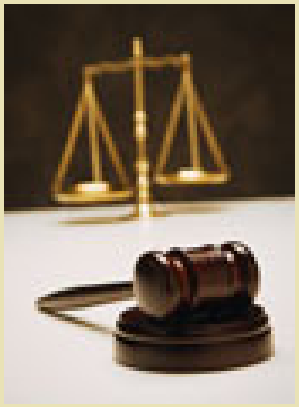
Security Challenges

- EHRs with limited security features/capabilities make it difficult to comply with some of the standards in the Security Rule



HIE Challenges

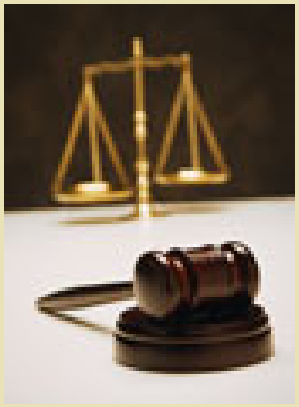
- Lack of broadband capabilities in rural/remote areas
- Lack of funds to invest
- Lack of expertise in smaller provider organizations. Some smaller providers have no IT personnel on staff
- EHR systems who don’t communicate with each other
- Developing a business model that's sustainable, that meets 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

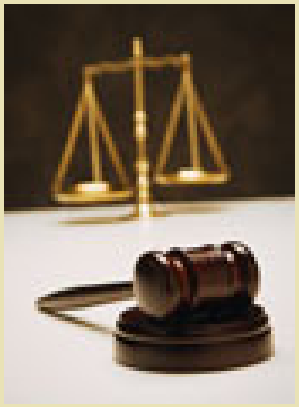
- Besides fears among competing healthcare providers sharing data about one's patients, other worries include whether a healthcare provider will be somehow dragged into a negative public spotlight or be liable if one of their HIE partners experiences a data breach



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

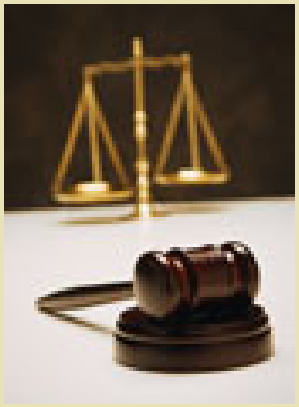
- If an HIE loses a big player over issues involving trust or secure data access and exchange, sustainability will be compromised



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

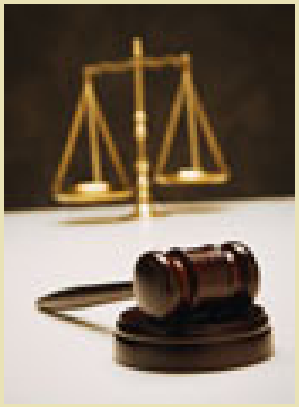
- That highlights the importance of a culture of compliance which is supported by ongoing education, auditing and monitoring, and ensuring there are consequences for non-compliance



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 a significant number of patients opt out of allowing you to disclose their electronic PHI, you will not only experience operational inefficiencies but it will be difficult to impossible to gather the information necessary to evaluate the performance of the integrated effort



QUESTIONS?

Tim Timmons
Corporate Integrity Officer
Greater Oregon Better Health Initiative

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