Health Information Exchanges: Evolving Legal and Regulatory Challenges

Evaluating HIE Models, Navigating Complex State and Federal Laws, and Negotiating Contracts With Vendors

Tuesday, November 20, 2012

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today’s faculty features:

Stephen P. Nash, Partner, Patton Boggs, Denver
Melodi M. (Mel) Gates, Patton Boggs, Denver

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Tips for Optimal Quality

**Sound Quality**
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory and you are listening via your computer speakers, you may listen via the phone: dial **1-866-370-2805** and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

**Viewing Quality**
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
Continuing Education Credits

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

• In the chat box, type (1) your company name and (2) the number of attendees at your location
• Click the word balloon button to send
Health Information Exchanges (HIE): Evolving Legal and Regulatory Challenges

Stephen P. Nash, Partner
snash@pattonboggs.com, (303) 894-6173
www.pattonboggs.com/snash

Melodi (Mel) Mosley Gates
mgates@pattonboggs.com, (303) 894-6111
www.pattonboggs.com/mgates
Agenda

• Introduction
  – Definitions, History, Current Environment, Scenarios, Roles & Applicable Law

• Health Information Exchange (HIE) Models
  – Four Key Perspectives & Selection Criteria for Participants and HIEs

• Legal & Regulatory Issues
  – Federal and State Considerations, Challenges to Multistate HIE

• Nationwide HIE
  – Evolution, Why Engage, Technology Considerations & Legal Requirements

• Resources
INTRODUCTION
What is Health Information Exchange?

• Health Information Exchange (HIE) refers to…
  – Technology that allows disparate (or the same) Electronic Health Record (EHR) systems to exchange information in a standardized manner, upon request (query) or through automated means (push or “Direct” exchange).
  – An actual data transaction between two or more parties.
  – The organization that implements, operates and maintains such capabilities.

• HIE technology may be provided using stand-alone tools, integration with existing EHR systems or both.
History

• As EHR systems emerged, the need for interoperability became clear, and pockets of data exchange arose within and across organizations.
• In 2004, by Executive Order, President Bush established the position of National Health Information Technology Coordinator and called for the development of “a nationwide interoperable health information technology infrastructure.”
• Enacted in 2009, as part of ARRA (the “Stimulus Act”), among other things, the Health Information Technology for Economic and Clinical Health (HITECH) Act:
  (1) Established the Office of the National Coordinator for Health IT (ONC);
  (2) Authorized Federal Advisory Committees for HIT Policies and Standards;
  (3) Provided for grants under the State Health Information Exchange (State HIE) Cooperative Agreement Program; and
  (4) Created the Meaningful Use program to incentivize provider implementation of EHR systems.
• Jumping ahead … in 2012, Stage 2 Meaningful Use rules require that providers demonstrate significant, actual interoperability and HIE capabilities by 2014 to receive incentive payments.
Current Environment

- HHS/ONC has awarded over $547 million in grants to 56 states, eligible territories and qualified State Designated Entities (SDE) under the State Health Information (State HIE) Exchange Cooperative Agreement Program.*
- Both Public and Private HIEs are now available and operating in a number of states, with a recent survey reporting 166 confirmed regional, state and local initiatives.**
- Over 30 organizations currently participate in the Nationwide Health Information Network (now known as the eHealth Exchange).***
- Records for millions of patients are available to authorized users – but we are still in early stages of adoption and deployment.

* See ONC’s State HIE Cooperative Program overview at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__state_health_information_exchange_program/1488.
Health Information Exchange (HIE) Scenarios

• Common HIE Scenarios
  – Data sharing between primary care physicians and specialists, including referrals;
  – Distribution of lab tests, imaging and other data from hospitals and independent suppliers (e.g., national labs) to physician practices; and
  – Data query capabilities for emergency room providers to learn about a patient’s history and conditions.
Health Information Exchange (HIE) Scenarios

• Emerging HIE scenarios
  – Increasing focus on automated (event-triggered) data exchanges.
  – Some examples include:
    • Automated public health reporting (e.g., newborn screening, immunization records, disease reporting);
    • Automated data routing for information regarding hospital admissions, discharges and transfers (ADTs);
    • Transmission of continuity of care documents;
    • Patient access to clinical information; and
    • Data analytics through aggregation and reporting.
Roles

• Visualize an **HIE** as a hub-and-spoke model.
  – An HIE acts as the “hub” brokering data exchanges among **HIE Participants** (the “spokes”).
  – Efficiency is increased by creating a network in place of individual point-to-point connections.
  – The level of data maintained and stored by the HIE varies.
  – HIEs interconnect with other HIEs to form larger networks.

• HIE Participants may be **Data Senders**, **Data Receivers** or both.

• HIEs typically utilize **Technology Vendors** to implement, operate and maintain the HIE.
  – Traditional and cloud computing implementations can be used to support HIEs.
Applicable Law

• Privacy and Data Security
  – Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  – Health Information Technology for Economic and Clinical Health (HITECH) Act
  – Implementing regulations (for HIPAA & HITECH)
  – Other regulations such as those regarding substance abuse and genetic information

• Technical Standards and Reporting Requirements
  – Meaningful Use Certification Regulations
  – State HIE Cooperative Agreement Program Requirements
  – Clinical Laboratory Improvement Amendments of 1988 (CLIA)

• State-specific Laws
  – Privacy and data security statutes, including medical records confidentiality/patient privacy, breach notification and patient consent
HIE Models
Health Information Exchange Models

- HIEs Models come in various forms and may be understood from four key perspectives, according to:
  - The kind of **ORGANIZATION** that implements and operates the HIE;
  - The **PURPOSES** for which information may be exchanged;
  - The **COMMUNITY** amongst which information is shared; and
  - The **CONSENT** model employed regarding the level of control patients may exert over access to and distribution of their EHRs through the HIE.

- Each HIE **trust community** makes choices regarding the four perspectives, and those decisions impact capabilities and risks for all of an HIE’s Participants (and the HIE itself).
Organization Perspective

- HIEs may be implemented by
  - Public Entities;
  - Private Entities; or
  - Public-Private Partnerships.

- The type of organization may impact available resources, contracting considerations and risks, including:
  - HIE Capabilities;
  - Sustainability;
  - Longevity; and
  - Legal Limitations.
Purpose Perspective

• HIEs may be implemented to share information for one or many purposes, such as
  – Patient treatment only;
  – Treatment, payment and health care operations;
  – Patient access to clinical information;
  – Public health functions; or
  – Data analytics.

• The data sharing purposes supported by an HIE will likely impact risk levels, as well as technical complexity and flexibility.
Community Perspective

- HIEs are typically established to serve a particular community of Participants.
  - For example:
    - Providers within a particular health system or those who use a particular EHR system;
    - A local or regional community of providers; or
    - A statewide community;

- HIEs may also support data exchanges with other HIEs (HIE-to-HIE) on behalf of their Participants.
  - For example:
    - To expand across a broader geographic area served by one or more other HIEs;
    - To accommodate migration of patients between communities (e.g., across state lines for specialist services and hospitals); or
    - To participate in the Nationwide Health Information Exchange (now known as the “eHealth Exchange”) that supports a wide community, including several federal agencies.
Consent Perspective

• The consent model an HIE chooses directly impacts the level of control a patient may exert over how information is shared.

• Typical models include:
  – No consent
  – Opt-out
    • Opt-out with exceptions or granular consent
  – Opt-in
    • Opt-in with exceptions or granular consent

• The consent model chosen is typically a reflection of state law, the values of a particular community or HIE, and the stage of HIE development at which patient groups are engaged.
Selection Criteria (HIE Participants)

• Providers that are considering whether to participate in an HIE should first examine their own objectives and values for each of the four key perspectives.
• HIE choices may be limited, based on communities served and technology capabilities.
• Some elements to consider include:
  – What the potential HIE Participant hopes to accomplish by joining an HIE (e.g., the desired functions both now and in the future);
  – Other information exchange options that may be available (if any);
  – Technology compatibility;
  – Patient population alignment;
  – Specific data use purposes supported by the HIE;
  – The terms and conditions offered by the HIE; and
  – Resources available to the HIE, including its plan for long-term viability.
Selection Criteria (HIEs)

- Organizations that are considering whether to develop, maintain and operate an HIE should examine their own views of the four key perspectives and the views of their likely participants.
- A proactive and transparent review allows a potential HIE to establish organizational values and credibility as it seeks to build a trust community.
- Some elements to consider include:
  - Desired data use purposes and consent model(s);
  - Competitive bidding processes for technology selection;
  - How well particular technology vendor(s) are able to integrate with the EHR systems used by potential HIE participants;
  - Other HIEs that are likely to be competitors and/or targets for HIE-to-HIE interactions; and
  - Whether to follow a traditional deployment model (i.e., build a data center and other infrastructure) or leverage a cloud-based implementation model.
Legal & Regulatory Issues
Applicable Laws & Regulations
Privacy and Data Security – HIPAA/HITECH

• The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act and the regulations promulgated thereunder, set requirements for privacy, security, and breach notification.

• The HITECH Act defines HIEs as “Business Associates” under the HIPAA regulatory regime.
  – Technology vendors are likely to be HIPAA subcontractors (i.e., downstream business associates).

• Heightened enforcement climate exists today (e.g., audits, mandatory breach notification, enforcement actions).

• HITECH-driven updates to the regulations are still pending and may (will!) have significant impacts.
Privacy and Data Security – 42 CFR Part 2 (Substance Abuse)

- Maintained by the HHS/Substance Abuse and Mental Health Services Administration (SAMHSA) regarding confidentiality for patient records held by federally-supported substance abuse programs.
  - Pose additional challenges for health information exchange, particularly in the area of behavioral health integration.
  - Regulations call for specific, detailed patient consent for data use or disclosure.
Technical Standards and Reporting Requirements

• Meaningful Use Certification Regulations
  – Lay out standards for EHR systems, including data protocols and information exchange functions.

• State HIE Cooperative Agreement Program
  – Sets requirements and standards for HIEs supported under the grant program.

• Clinical Laboratory Improvement Amendments of 1988 (CLIA)
  – Requires lab result reports to meet certain specifications, including those provided through electronic means.
  – HIEs and HIE Participants may be impacted when using an HIE to transport/receive “reports of record.”
State-Specific (Privacy & Security)

- HIPAA provides a floor for patient privacy.
- HITECH grants HIPAA enforcement authority to state attorneys general.
- States can (and do) impose additional requirements that may impact health information exchange.
- Examples of state-specific statutes include:
  - Medical records confidentiality, especially for highly sensitive information (e.g., HIV results);
  - Behavioral health records confidentiality;
  - Variations in how lab testing results may be shared; and
  - Patient access to records.
- General state-specific statutes regarding data breach notification and data protection may also apply.
State-Specific (HIE Consent)

• Several states have enacted statutes regarding establishment of their state designated HIEs.
• In some cases, state statutes and/or regulations dictate the consent model HIEs must use.
• For example:
  – Delaware calls for patients to be allowed to opt-out (1-100-102 Del. Code Regs. §§ 1.0-8.0);
  – Rhode Island dictates an opt-in model (256 R.I. Gen. Laws § 5-37.7-4); and
HIE Participant Considerations
Data Senders & Receivers

- HIE Participants may be Data Senders, Data Receivers or both.
- Participation in an HIE does not alleviate any of an organization’s regulatory obligations regarding how protected health information is used or disclosed.
- Potential HIE Participants must engage in reasonable due diligence before participating in an HIE.
  - Alignment with data uses and consent model;
  - Impact to compliance programs and office workflow;
  - Risks and benefits of becoming part of a trust community (weakest link provider issue); and
  - Opportunities for risk allocation and exposure management through HIE agreements.
Covered Entity Obligations

- HIE Participants are typically HIPAA Covered Entities.
- Some key issues include:
  - How the HIE helps Participants manage their obligations regarding data disclosures and uses (e.g., treatment, payment and health care operations; patient authorizations);
  - The Minimum Necessary rule and its impact on HIEs (and their Participants), especially those that go beyond sharing data for treatment purposes;
  - Managing (or avoiding) sharing of especially sensitive information that may be further limited by HIPAA, HITECH or state law; and
  - Terms of the Business Associate Agreement executed between the HIE and its Participants regarding permitted disclosures and uses of protected health information (e.g., de-identification, aggregation).
Participant Agreement Risks & Issues

• Because they create a trust community of Participants, HIEs typically call for standardized Participant Agreements.
  – Sometimes called “Data Use Agreements.”
  – Negotiability of terms & conditions may (and perhaps should) be limited.
  – Potential HIE Participants should consider an HIE’s other current and anticipated Participants, along with costs and capabilities.
  – Traditional implementation and software licensing models should be contrasted with software-as-a-service offerings, including their financial impacts (e.g., capital/expense investments, tax implications).

• Potential HIE Participants should be especially mindful of terms & conditions regarding
  – Data ownership;
  – Data architecture and storage methods;
  – Data integrity, safeguards and auditing;
  – Data uses including analytics, de-identification, aggregation and reporting;
  – Technology standards, protocols and features;
  – EHR integration capabilities and vendor management;
  – Breach notification protocols; and
  – Risk apportionment and insurance coverage.
Compliance Program Impacts

• HIE Participants should consider and account for potential changes to their
  – Regular risk assessments related to protected health information;
  – Employee training;
  – Patient-related processes and workflow, including those regarding consent, access and requests for limitations; and
  – Risk management strategies, including cyberinsurance.
HIE Considerations
Business Associate Obligations

• Under the HITECH Act, HIEs are typically HIPAA Business Associates.

• HIEs must be prepared to implement and maintain a strong HIPAA compliance program both in light of HITECH’s requirements and to promote a healthy trust community.

• Technology vendor governance is critical, along with regular risk assessment and well-defined processes for audit logging (and reviews), incident response management and compliance management.
Participant Agreements

• Participant agreement development provides the foundation for and should reflect a shared understanding of the HIE’s trust community.
• HIEs should
  – Consider current and future capabilities when crafting provisions related to data use and disclosures that will
    • Encourage flexibility as technologies evolve;
    • Support changes without renegotiation or costly agreement maintenance; and
    • Provide Participants with confidence and trust that their data is used and disclosed in a responsible manner.
  – Recognize the limits of their role and allocate risk accordingly (e.g., data integrity, use of information provided, errors and omissions, breach response).
  – Consider offering a variety of implementation models, including both traditional software licensing and software-as-a-service to meet differing Participant needs.
• Pricing models should
  – Reflect the value proposition offered to different categories of HIE Participants using various information exchange methods (e.g., EHR integration, Direct exchange, query capabilities, automated data routing).
  – Recognize current and anticipated costs as technologies and user requirements evolve.
Business Associate Agreements

• Because HIEs are Business Associates under HIPAA to most (if not all) of their Participants, Business Associate Agreement (BAA) development and maintenance provides an opportunity to streamline compliance and foster trust among Participants.

• HIEs should
  – Standardize BAAs and leverage the trust community to simplify compliance and avoid special cases.
  – Consider creating a multi-layered agreement model with Participants and technology vendor(s) to simplify agreements and enhance transparency.
Benefits of HIE Policies

• A strong, multi-stakeholder HIE policy process can provide significant benefits in flexibility and transparency while encouraging HIE Participant engagement and ownership for trust community values.
  – To be effective, policies should connect broad contract terms to detailed HIE operational procedures.

• Participant Agreements should incorporate policies by reference and provide options should material disagreements over policy positions arise.

• Policy maintenance and governance processes should be formal, well-documented and inclusive.

• HIEs should recognize that policy stakeholders may include community members, patient representatives and others beyond HIE Participants.
Technology Vendor Pitfalls

• Technology selection and a strong, ongoing partnership with the chosen vendor may be the critical success factor for HIEs.
• HIEs should consider the pros and cons of traditional implementation models versus cloud computing, including the use of private clouds to promote security and privacy.
• Some HIE Participants may prefer traditional software licensing over software-as-a-service models, so flexibility in client models should be preserved regardless of the infrastructure model.
• Technology vendor service agreements must balance incentives for new feature development and regulatory compliance (especially as regimes evolve) with solid ongoing service levels.
  – EHR vendor interfaces can be especially challenging to HIE growth and deployment.
  – HIEs should develop shared risk/reward models with their technology vendors to encourage standardization and process maturity.
  – Service agreements should specify privacy and security requirements, responsibilities and audit obligations.
The “Big Picture”

TRUST COMMUNITY

HIE

Participants
- Physician Practice
- Hospital
- Labs, Others

Participant Agreements

Services Agreement

Technology Vendor(s)

- Single Multi-layered Business Associate Agreement
- Participants (Covered Entities)
- HIE & Technology Vendor(s) (Business Associates)

• DURSA
• Individual HIE-to-HIE Agreements

HIE

HIE

HIE

...
Challenges to Multistate HIE
Challenges to Multistate HIE

• Differences in state-specific privacy and confidentiality statutes (e.g., consent models, disclosure limitations) can create technical and process challenges to multistate health information exchange.
  – Data provenance tagging and granular consent provide potential technology solutions.
  – Supporting processes to manage differences still must be implemented to complement technology capabilities (where they are available).

• ONC is sponsoring an E-Consent pilot program to improve patient education and capture consent choices online.
Nationwide HIE
Evolution

• The nationwide health information network has been variously known as the NHIN, the NwHIN and is now called the “eHealth Exchange (EHE).”
  – Recently transitioned to a public-private partnership, Healtheway, Inc.

• Conceptually, the EHE may be broadly defined as “the set of standards, specifications and policies that enable the secure exchange of health information over the Internet.”*

• The EHE leverages Internet concepts to promote standards-based interoperability and communications.
  – Network-of-networks model

Why Engage?

- Provides broad connectivity and query potential for a mobile population.
- Is the mechanism for health information exchange with certain federal agencies, including the Department of Veterans Affairs.
- May avoid the necessity of individually negotiated (and maintained) HIE-to-HIE agreements.
- Creates a large-scale trust community that can be leveraged by individual HIEs and their Participants.
Technology & Legal Requirements

- Participants (typically HIEs or large organizations) must be prepared to support widely-accepted technology standards.
- Legal duties and obligations are dictated by a multi-party participation (data use) agreement known as the Data Use and Reciprocal Support Agreement (DURSA).
- Key question for HIE Participants →
  - Is your HIE a party to the DURSA and/or do they plan to join the agreement?
- Key question for HIEs →
  - Are you willing and prepared to join the DURSA?
Key Elements of the DURSA

• “The Agreement reflects consensus … regarding the following issues:
  – Multi-Party Agreement
  – Participants Actively Engaged in Health Information Exchange
  – Privacy and Security Obligations
  – Requests for Information Based on a Permitted Purpose
  – Duty to Respond
  – Future Use of Data Received from Another Participant
  – Respective Duties of Submitting and Receiving Participants
  – Autonomy Principle for Access
  – Use of Authorizations to Support Requests for Data
  – Participant Breach Notification
  – Mandatory Non-Binding Dispute Resolution
  – Allocation of Liability Risk**

• New participants must execute a joinder agreement.
• Governance and maintenance is provided by a representative Coordinating Committee.
• Participants who are not HIPAA Covered Entities, Business Associates or Government Entities (subject to applicable laws such as the Privacy Act) agree to act as a Covered Entity with respect to HIPAA regulations.

Resources
• Feel free to contact us with your questions!
• The Office of the National Coordinator (ONC) provides extensive information regarding research, standards and programs related to Health Information Exchange and other Health IT initiatives at http://healthit.hhs.gov.
• Information regarding the eHealth Exchange (EHE) and the DURSA is available on the Healtheway, Inc. site at http://healthewayinc.org/.
• The eHealth Initiative monitors current HIE activities and provides an annual survey, along with toolkits and other research at http://www.ehealthinitiative.org/.
Thank you for your attention.

Stephen P. Nash, Partner
snash@pattonboggs.com
www.pattonboggs.com/snash
(303) 894-6173
1801 California Street, Suite 4900
Denver, Colorado USA 80202

Melodi (Mel) Mosley Gates
mgates@pattonboggs.com
www.pattonboggs.com/mgates
(303) 894-6111
1801 California Street, Suite 4900
Denver, Colorado USA 80202