

Selecting & Using a Health Information Exchange

Understand Services and Functionality

Before selecting a health information exchange (HIE), it is important to look at the advantages and disadvantages the provider brings to the table. HIE availability and sophistication varies by state and region and services vary with each HIE, but some of the possible functionalities for HIE initiatives include connectivity to electronic health records (EHRs), health summaries for continuity of care and clinical decision support tools.

While researching potential HIEs, make sure to keep track of changing concepts, labels, policies, and organizations (e.g., HIMSS "[What is Health Information Exchange?](#)").

One such organization—the [Sequoia Project's eHealth Exchange](#) is a rapidly growing network of exchange partners who securely share clinical information over the internet in the US, with a standard approach. EHealth Exchange participants are able to securely share health information with each other, without additional customization and one-off legal agreements by leveraging a set of standards and governance. The eHealth Exchange connectivity spans across all 50 states and is now the largest HIE Network in the United States.

As a founding member of [The Sequoia Project](#) (previously Healthway), a non-profit 501(c)(3), the AMA is dedicated to the implementation of secure, interoperable nationwide HIE and is supporting these efforts and participates on the boards of both the eHealth Exchange and [Carequality](#).

Review Financial Costs

Physicians need to carefully look at the direct and indirect costs of participating in an HIE.

Things to consider when participating in an HIE:

- Fees may be charged per transaction, monthly, annually or a combination of transaction and subscription fees.
- Fees may change over time, particularly if the HIE is initially dependent upon federal funds. Inquire about how the HIE notifies physicians about price changes.
- Cost of upgrading the office's information technology systems to meet the HIE system requirements.
- Costs of lost revenue and productivity during the HIE implementation phase.

Consider Liability Concerns

The risks and liability of joining an HIE is an evolving legal field. Physicians may face complex questions and uncertainties related to liability. Primary liability concerns related to HIEs include:

- Liability for data storage and management
- Liability for data accuracy and completeness
- Liability for decisions made with inaccurate data
- Duty to review
- Reproducibility of data available in the HIE at a particular moment in time
- Availability of audit and access logs

Research any potential HIE partner and clarify special liability protection issues related to participation prior to signing a contract. Make sure to consult with legal counsel before signing an HIE contract. Physicians should also discuss the malpractice coverage in relationship to HIE participation with their insurance agent.

Data Access

Patient data access and use can vary considerably between HIEs. It is critical for physicians to establish who has access to data within the HIE and how the information will be used prior to signing an HIE contract.

Laws and Regulations

Federal and state laws and regulations apply to HIE activities, including the privacy and security of patient's health care information. The HITECH Act established the federal criteria for [Meaningful Use](#) of health information technology, while some states have legislated the privacy and security of information transmitted by or through an HIE. It is important for physicians to understand the implications of HIE regulations at all levels.

HIPAA Implications

Although HIEs are generally not covered entities under the Health Insurance Portability and Accountability Act (HIPAA) they are considered to be business associates of HIPAA covered entities. Any system used by an HIE must comply with the privacy and security provisions of HIPAA.

HIPAA may be superseded by more stringent state privacy laws and regulations. Physicians should ask about a potential HIE partner's privacy and security safeguards and how data breaches will be managed. See the [AMA's HIPAA toolkit](#) for additional information and resources.

Handling Sensitive Patient Data

Sensitive patient information can be exchanged via health information exchanges. Special patient consent may be required to share certain types of sensitive health records (e.g., HIV/AIDS status, sexually transmitted diseases, mental health) within the HIE and it must comply with HIPAA requirements. Sensitive health information may not be included in the patient's records from the HIE if the patient has not provided the necessary consent.

Patient Notification

Patient notification regarding HIE participation usually happens via the provider's HIPAA-mandated Notice of Privacy Practices. It provides information about how the provider will use and disclose the patient's health information, as well as the provider's obligations to protect this information.

The patient notification could be an opt-in or opt-out model. In opt-in HIE models, patients must give consent to have their data included in the HIE. In opt-out systems, patients' data are automatically included in the HIE, but patients may choose to withdraw from HIE participation.

LINKS

[AMA/HIMSS Podcast: "Episode #5 - Physician engagement with HIE"](#)

[AMA/HIMSS Podcast: "Episode #8 - Information exchange: HISPs and HIEs"](#)

[How digital health empowers physicians and patients](#)

[Understanding Meaningful Use criteria](#)

[NORC's final report on Provider Experiences with HIEs](#)

[Sequoia Project's strategy for better patient matching](#)

[Bipartisan Policy Center's whitepaper on Clinician Perspectives on Electronic Health Information Sharing for Transitions of Care](#)

[State Health IT Policy Levers Compendium](#)

[George Washington University Health Information and the Law project](#)