

Direct

The Direct Project¹ is the set of standards, policies, and services that enable simple, secure transport of health information between health care participants (such as providers and laboratories) who know each other and already have a relationship of trust. The Direct Project enables standards-based exchange of health information in support of core Stage 1 Meaningful Use (MU) measures. This can include communication of summary care records, referrals, discharge summaries, and other clinical documents in support of continuity of care and medication reconciliation, as well as communication of laboratory results to ordering providers.²

Brief Description of Interchange Attributes	Data Transformation and Normalization Attributes	Role of Health Information Exchanges (HIEs)	Advantages	Disadvantages	Standards in Use
<ul style="list-style-type: none"> Simple, secure, scalable, standards-based way for participants to “push” encrypted health information directly to known, trusted recipients over the Internet. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> Can vary. Health information exchanges (HIEs) can serve as Health Information Service Providers (HISPs) to facilitate communication, or providers can subscribe to market-based services. Some states provide these services as well. The important thing is to participate in a trust domain with intended data exchange partners. 	<ul style="list-style-type: none"> “Push” model supports Syndromic Surveillance paradigm well. Strong support from the Office of the National Coordinator for Health Information Technology (ONC) leading to broad adoption. Can support many different payloads. Supports integration into Electronic Health Record (EHR) systems or standalone interfaces such as a Web portal or e-mail client. Explicitly mentioned in Stage 2 Notice of Proposed Rulemaking (NPRM). 	<ul style="list-style-type: none"> Actual adoption not yet widespread. States require HISP infrastructure via contracted services or internal information technology (IT) support. Does not readily support message acknowledgement. 	<ul style="list-style-type: none"> Simple Mail Transfer Protocol (SMTP). Multipurpose Internet Mail Extensions (MIME). Integrating the Healthcare Enterprise Cross-Enterprise Document Reliable Interchange (IHE XDR) (optional). Public Key Infrastructure (PKI).

¹U.S. Department of Health and Human Services, State HIE Resources <http://statehieresources.org/>.

²Table: ISDS; Architectures and Transport Mechanisms for Health Information Interchange of Clinical EHR Data for Syndromic Surveillance, prepared by Noam H. Arzt, PhD, HLN Consulting, LLC.

HTTPS POST/REST

HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer (SSL) or HTTP Secure) uses SSL or Transport Layer Security (TLS) under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server, protecting against eavesdropping and man-in-the-middle attacks.

POST is one of many request methods supported by the HTTP protocol used by the Web. The POST request method asks a Web server to accept the data in the request message's body for storage.

REST³ (Representational State Transfer) is an approach for getting information content from a Web site by reading a Web page that contains an Extensible Markup Language (XML) file that describes and includes the desired content. For example, REST can be used to publish syndicated content. Periodically, the publisher activates a Web page that includes content and XML statements that describe the content. Subscribers only need to know the uniform resource locator (URL) for the page where the XML file is located, read it with a Web browser, interpret the content using the XML information, and reformat and use it appropriately (perhaps in some form of online publication).²

Brief Description of Interchange Attributes	Data Transformation and Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in Use
<ul style="list-style-type: none"> Common form of transport used by Web browsers to send data to Web services. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> Fairly simple to implement. 	<ul style="list-style-type: none"> Sender and receiver must agree on payload structure, which is likely to be nonstandard. 	<ul style="list-style-type: none"> Hypertext Transfer Protocol Secure (HTTPS). SSL/TLS.

MLLP

Minimal Lower Layer Protocol (MLLP) defines the leading and trailing delimiters for a Health Level Seven (HL7) message. These delimiters help the receiving application determine the start and end of an HL7 message that uses Internet Protocol network as transport.²

Brief Description of Interchange Attributes	Data Transformation and Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in Use
<ul style="list-style-type: none"> Relatively simple form of message transport over Transmission Control Protocol/Internet Protocol (TCP/IP). 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> Simple, easy to implement. 	<ul style="list-style-type: none"> No security features—requires virtual private network (VPN) for security. 	<ul style="list-style-type: none"> TCP/IP. SSL/TLS.

³TechTarget SearchSOA

PHIN MS

The Public Health Information Network Messaging System (PHIN MS) is software that allows public health organizations to send and receive encrypted data over the Internet to public health information systems securely. The PHIN Messaging and Vocabulary Program works with standards organizations such as HL7 and Healthcare Information Technology Standards Panel (HITSP) to produce message specifications and mapping guides, so that public health professionals across the country use the same language and a single set of codes to represent public health concepts.²

Brief Description of Interchange Attributes	Data Transformation and Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in Use
<ul style="list-style-type: none"> CDC-created strategy for public health data exchange. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> May be an intermediary or connection directly between the source and destination of the data. 	<ul style="list-style-type: none"> Implemented and supported by Public Health Agencies (PHAs) in several states, especially with hospital partners. 	<ul style="list-style-type: none"> Complex to implement, especially for small organizations. Few vendors have experience with it. 	<ul style="list-style-type: none"> Electronic Business Extensible Markup Language (EBXML). SSL/TLS.

SFTP

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and transfer over a Secure Shell (SSH) data stream. It is part of the SSH protocol. Its functionality is similar to that of FTP, but SFTP uses SSH to transfer files. SFTP requires the client user to be authenticated by the server, and the data transfer must take place over a secure channel (SSH). It allows a wide range of operations to be performed on remote files—such as resuming halted transfers, directory listings, and remote file removal—acting somewhat like a remote file system protocol.²

Brief Description of Interchange Attributes	Data Transformation and Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in Use
<ul style="list-style-type: none"> Internet standard for point-to-point interactive or batched secure file transfer. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> None. 	<ul style="list-style-type: none"> Simple to use; no firewall or network transmission issues. Secure and encrypted. 	<ul style="list-style-type: none"> Most implementations use interactive clients, while the goal is for a more transparent user experience. 	<ul style="list-style-type: none"> Secure File Transfer Protocol (SFTP).

Web Services

A service-oriented architecture (SOA)³ is the underlying structure supporting communication between services. The SOA defines how two computing entities, such as programs, interact to enable one entity to perform a unit of work on behalf of another entity. Service interactions are defined using a description language. Each interaction is self-contained and loosely coupled, so that each interaction is independent of any other interaction.²

Brief Description of Interchange Attributes	Data Transformation and Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in Use
<ul style="list-style-type: none"> • SOA-based strategy for enabling two systems to interoperate securely. 	<ul style="list-style-type: none"> • May be included as a companion service. 	<ul style="list-style-type: none"> • May be an intermediary or connection directly between the source and destination of the data. 	<ul style="list-style-type: none"> • Becoming more favored by Electronic Health Record (EHR) system vendors. • Secure, flexible, and powerful; supports same security features as HTTPS POST plus additional features of WSSecurity and Security Assertion Markup Language (SAML) assertions. • Basis of both Integrating the Healthcare Enterprise (IHE) and Nationwide Health Information Network (NwHIN) implementations. • Explicitly mentioned in Stage 2 Notice of Proposed Rulemaking. 	<ul style="list-style-type: none"> • Data payload defined by a Web Services Description Language (WSDL) document, which may or may not be standard. • May be somewhat complex to implement. 	<ul style="list-style-type: none"> • Simple Object Access Protocol (SOAP). • SSL/TLS. • XML. • Nationwide Health Information Network (NwHIN) CONNECT.