

Direct

The Direct Project¹ is the set of standards, policies and services that enable simple, secure transport of health information between healthcare participants (e.g., providers, labs) 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 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 / Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in use
Simple, secure, scalable, standards based way for participants to “push” encrypted health information directly to known, trusted recipients over the Internet	None	Can vary. HIEs can serve as Health Information Service Provider (HISP) to enable/facilitate communications or providers can subscribe to market based services. Some states provide these services as well. Important thing is to participate in a trust domain with intended data exchange partners.	<ul style="list-style-type: none"> • “Push” model supports SS paradigm well • Strong ONC support leading to broad adoption • Can support many different payloads • Supports integration into EHR systems or standalone interfaces (e.g., web portal or email client) • Explicitly mentioned in Stage 2 NPRM 	<ul style="list-style-type: none"> • Actual adoption not yet widespread • States require HISP infrastructure, via contracted services or internal IT support • Does not readily support message acknowledgement 	<ul style="list-style-type: none"> • SMTP/MIME • IHE XDR (optionally) • PKI

¹U.S. Department of Health & Human Service, 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 (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks.

POST is one of many request methods supported by the HTTP protocol used by the World Wide Web. The POST request method is designed to request that a web server accepts the data enclosed 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 designated Web page that contains an XML (Extensible Markup Language) file that describes and includes the desired content. For example, REST could be used by an online publisher to make syndicated content available. Periodically, the publisher would prepare and activate a Web page that included content and XML statements that described the content. Subscribers would need only to know the URL (Uniform Resource Locator) for the page where the XML file was located, read it with a Web browser, interpret the content data using the XML information, and reformat and use it appropriately (perhaps in some form of online publication).

⁴

Brief Description of Interchange Attributes	Data Transformation / Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in use
Common form of transport used by web browsers to send data to web services	None	None	<ul style="list-style-type: none">Fairly simple to implement	<ul style="list-style-type: none">Sender and receiver need to agree on payload structure which is likely to be non-standard	<ul style="list-style-type: none">HTTPSSL/TLS

³TechTarget SearchSOA <http://searchsoa.techtarget.com/>

⁴ Table: 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

MLLP

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

5

Brief Description of Interchange Attributes	Data Transformation / Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in use
Relatively simple form of message transport over TCP/IP	None	None	<ul style="list-style-type: none">• Simple, easy to implement	<ul style="list-style-type: none">• No security features – requires VPN for security	<ul style="list-style-type: none">• TCP/IP• SSL/TLS

⁵ Table: ISDS; Architectures and Transport Mechanisms for Health Information Interchange of Clinical EHR Data for Syndromic Surveillance, prepared by Noam H. Arz, PhD, HLN Consulting, LLC

PHINMS

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

⁶

Brief Description of Interchange Attributes	Data Transformation / Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in use
CDC-created strategy for public health data exchange	None	May be an intermediary or connection maybe directly between the source and ultimate destination of the data	<ul style="list-style-type: none"> • Implemented and supported by PHAs in a number of states, especially with hospital partners 	<ul style="list-style-type: none"> • Complex to implement, especially for small organizations • Future of product uncertain • Few EHR-S vendors have experience with it 	<ul style="list-style-type: none"> • ebXML • SSL/TLS

⁶ Table: 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

SFTP

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. The functionality of SFTP is similar to that of FTP. However, SFTP uses SSH to transfer files. SFTP requires that the client user must 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, acting somewhat like a remote file system protocol. SFTP allows operations such as resuming from halted transfers, directory listings and remote file removal.

7

Brief Description of Interchange Attributes	Data Transformation / Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in use
Internet standard for point-to-point interactive or “batched” secure file transfer	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 goal is for a more user transparent experience	<ul style="list-style-type: none">• SFTP

⁷ Table: 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

Web Services

A service-oriented architecture (SOA)⁸ is the underlying structure supporting communications between services. SOA defines how two computing entities, such as programs, interact in such a way as 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.

9

Brief Description of Interchange Attributes	Data Transformation / Normalization Attributes	Role of HIEs	Advantages	Disadvantages	Standards in use
SOA-based strategy for enabling two systems to interoperate securely	May be included as a companion service	May be an intermediary or connection maybe directly between the source and ultimate destination of the data	<ul style="list-style-type: none"> • Becoming more favored by EHR system vendors • Secure, flexible, and powerful; supports same security features as HTTPS POST plus additional features of WSSecurity and SAML assertions • Basis of both IHE and NwHIN implementations • Explicitly mentioned in Stage 2 NPRM 	<ul style="list-style-type: none"> • Data payload defined by a WSDL document which may or may not be standard • May be somewhat complex to implement 	<ul style="list-style-type: none"> • SOAP • SSL/TLS • XML • NwHIN CONNECT

⁸ TechTarget SearchSOA <http://searchsoa.techtarget.com/>

⁹ Table: 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

