



HTTPS

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.

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.

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.¹

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; ADHS has additional firewall security. file transfers are 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).

¹Table: 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. Original source document can be found at: <http://www.cdc.gov/cancer/npcr/pdf/TransportOptions.pdf>