

POSTER ABSTRACTS

9th Annual HMO Research Network Conference

April 1-2, 2003 Denver, CO

Information Technology

24

Transferring Confidential Research Data: Using a Secure Web-Based File Transfer Protocol

Mark C. Hornbrook, PhD, Center For Health Research, Kaiser Permanente, Northwest/Hawai'i

Gary C. Ansell, BS, Center For Health Research, Kaiser Permanente, Northwest/Hawai'i

Donald J. Bachman, MS, Center For Health Research, Kaiser Permanente, Northwest/Hawai'i

Chris Eddy, BS, Center For Health Research, Kaiser Permanente, Northwest/Hawai'i

Mike Thornton, Center For Health Research, Kaiser Permanente, Northwest/Hawai'i

Background: The Health Insurance Portability and Accountability Act (HIPAA) significantly increased the required level of protection of personal health information. In many studies, it is necessary to move research data from one site to another. In this paper, we describe a secure Web-based file transfer application we developed to increase the security of transmitting data from one physical location to another. This application uses e-commerce encryption and verification technology and standards to provide secure and rapid file transfers. This application transfers data for approved health care research (including sensitive data) from an approved user to an approved receiver using a secured Web site.

Methods: Confidentiality and security of the file transmissions are ensured using a combination of certificate authentication when clients connect to the host server, custom programming to secure individual access to forms and other documents, and Secure Sockets Layer (SSL) encryption to ensure that confidential data cannot be revealed even if packets were intercepted in transmission. Access is restricted to 128-bit key versions on Netscape and Internet Explorer, which provide a higher level of encryption than other browsers. Person-level user IDs and passwords and client certificates are required to log on.

Results: Over the past 14 months, the CHR has established about 150 users with client certificates, encompassing 24 research projects throughout the United States. Once access is approved, the user uploads a file to the Web site and the receiver logs onto the approved folder and file and downloads it. Notifying the receiver that the file will be posted at a specified time can minimize security risk exposure. The system automatically logs out a user after 15 minutes of nonuse.

Conclusions: Users have successfully and easily transferred 100MB files and larger. Most Institutional Review Boards that have been asked to approve use of the secure file transfer system has approved it. This successful application is being used by many multi-site studies. This method reduces the risk of inadvertent delivery to unintended location as well as the risk of interception by unauthorized users compared to other transfer modes.