CANOPY SECURITY FEATURES ENABLE HIPAA COMPLIANCE

Recent HIPAA regulations place stringent new requirements on healthcare providers to ensure the security and confidentiality of patient health information. Canopy is your key to compliance.

Privacy, security, integrity, and availability are key concerns when patient data are distributed over the Internet. Canopy Systems is firmly committed to helping you protect the confidentiality of patient information. The Canopy® solution enables healthcare organizations to readily comply with Health Insurance Portability and Accountability Act (HIPAA) regulations governing the use and disclosure of protected health information.

Unlike PC-based or client-server systems, Canopy is a secure, Web-based, ASP application. The Canopy solution handles the security procedures, intrusion defenses, and administrative and surveillance tasks dictated by HIPAA, while you concentrate on managing your patients. In addition, the Canopy solution helps ensure compliance for traditional paper-intensive processes that involve photocopying and faxing huge amounts of confidential patient data.

Canopy addresses security issues on multiple levels, including our Secure Data Center, two-factor user authentication, a comprehensive data access control system, and industry-standard encryption procedures. Canopy's security features provide a flexible, configurable tool to help you establish policies for user access. In addition, the Canopy solution creates a complete audit trail that documents each user session, including patient records created and modified.

Security features include:

- **Secure Data Center.** Canopy is housed at our state-of-the-art data center, which features rigorous controls for physical access, redundant high-speed Internet connections, backup generators, and secure off-site data backups. Sophisticated firewall devices guard against intrusion by filtering out network traffic that could be exploited by an intruder.
- **User IDs and Logins.** When a user connects to Canopy, the server requests a user ID and password, which are validated by the application software. A user's ability to view or edit data is controlled by his or her user ID and its associated user roles.
- **Virtual Private Network (VPN).** VPN access to Canopy can be configured using our industry-standard Cisco PIX firewall to create 3DES IPSec encrypted tunnel. This tunnel authenticates the origin of the network traffic (Hospital Network), in essence providing a different form of 2-factor authentication. Since this provides strong authentication, use of client certificates is optional.
- **Digital Certificates.** Installed on an individual computer, certificates provide a secure form of unique identifier that is difficult to forge.

CANOPY SYSTEMS, INC.™

PRODUCT

Certificates are issued by trusted third parties known as Certification Authorities, who digitally sign the certificate using their own private key. This protects the certificate against tampering and also vouches for the holder's identity. In addition, users must have their Canopy administrator's approval to use a certificate with their specific user ID. This creates a strong, two-factor mode of authentication for accessing Canopy over the public Internet.

- **User Roles.** Users of the system are assigned user roles, such as case manager and administrator, which are configurable for each healthcare organization. A user is authorized to view or edit specific data for specific patients, or administer Canopy configuration, according to user role.
- **Patient Data Access Control.** Similarly, patients are organized into groups that are configurable for each client organization. For example, patient groups may be established for a particular facility, a particular payor, patients in a disease population, etc. These groups allow you to establish permissions and policies that control the use of protected data within your organization.
- **Automated Audits.** Canopy keeps a detailed log of each user's session in Canopy to monitor and control use of the system.
- **Encryption.** For those using certificates, Canopy uses RSA public-key encryption during data transfers to ensure that only authorized people have access to documents, patient status information, and other key data. For those using VPNs, Canopy uses DES or 3DES encryption with IPSec as the transport.

For More Information ***on the security features of the Canopy solution, please contact Canopy Systems:***

[p] 1-800-757-1354
[w] www.canopysystems.com