



HIPAA COMPLIANCE AND SECURITY STATEMENT

At Crisalix, we care about the security of your personal information. Crisalix e-Stetix complies with the strictest privacy regulations in the world, including HIPAA guidelines. The system also uses Secure Sockets Layer (SSL), a data encryption technology, which ensures that data is unreadable during the transfer. The Crisalix e-Stetix system is designed to allow customers to meet their requirements under applicable US patient privacy laws, including HIPAA.

Storing data in the Crisalix e-Stetix system is often safer than storing it on a home computer system that is connected to the Internet. We use a three-tier architecture that puts the data behind three separate firewalls.

The Health Insurance Portability and Accountability Act (HIPAA) has two rules of importance for your practice as it relates to Crisalix: The Security Rule and the Privacy Rule that fall under a general HIPAA category known as the Administrative Simplification Act. Both rules have some influence on the transmission, storage and management of patient images.

Although Crisalix is not a covered entity and is thus not subject to the privacy and security provisions of the Health Insurance Portability and Accountability Act ("HIPAA"), we recognize the significant role that HIPAA has on our customers. Accordingly, we protect patient privacy and confidentiality in a manner that comports with HIPAA and other applicable laws and regulations. The Crisalix e-Stetix simulation system is utilized to transmit, store and manipulate digital images via the Internet that can contain PHI (patient identifiers, photos, etc.). We have prepared this statement to provide a brief overview of how the HIPAA Privacy and Security Rules pertain to 3D simulations.

Security Rule: The HIPAA Security Rule became effective on April 21, 2003. The Security Rule is intended to protect the confidentiality of medical information. The Security Rule establishes requirements that facilitate a medical practice's storage, maintenance and transmission of PHI in a "secure electronic environment." This involves administrative procedures and physical safeguards as well as technical measures to control and monitor access to PHI and to prevent unauthorized access to data during transmission.

Privacy Rule: The HIPAA Privacy Rule, which covers the use and disclosure of protected health information (PHI), became effective on April 14, 2001. It mandated that all practices had to be compliant with the Privacy Rule effective April 14, 2003.

The Privacy Rule requires that practices make reasonable efforts to limit the use and disclosure of such PHI by staff members to the "minimum necessary" to perform their duties. Practices

are also expected to minimize the likelihood of "incidental disclosures" to persons who have no legitimate need to view PHI. Further, practices must maintain a log of certain PHI disclosures that are not directly related to a patient's treatment.

Crisalix compiled some suggestions to help ensure that your practice manages patient images and related simulations in a responsible and HIPAA-compliant manner with Crisalix's e-Stetix:

- Securely store your passwords where other staff members or patients do not have access.
- Set up user accounts for your computers that require users to log in with a password.
- Always exit or log out of your Crisalix e-Stetix account when not using it.
- When using e-Stetix with of patients, use unique identifiers for patients that enhance privacy.
- Develop standard operating procedures (SOPs) requiring any use of the patients images functions to be documented.
- Maintain your laptop computer and digital camera in safe locations with limited access inside your practice.
- Maintain a copy of your Crisalix's Users Agreement (completed at the time of your e-Stetix subscription and available at www.Crisalix.com).

While there is no such thing as "HIPAA-compliant" 3D simulation software, Crisalix is making every effort to develop its products that integrate easily into a HIPAA-compliant practice and to assist our customers in complying with HIPAA.