Data Security

The American Red Cross is committed to donor and patient privacy, and we employ a variety of industry-standard measures to ensure that the donor and patient information entrusted to us is secure. This commitment to privacy applies to the orders hospitals place in Connect, the Red Cross's online order management system for hospitals.

Data Security and Availability

Connect uses a software application called BloodHub. BloodHub uses a variety of technologies and processes to safeguard confidential data. For example, all data submitted to Connect is encrypted during transit and at rest using encryption methods that meet the standards of the National Institute of Standards and Technology (NIST). Transmissions from the customer to the database are encrypted using TLS1.2, and data in the database is encrypted using AES-256.

In addition, Connect uses strong measures to prevent and detect intrusions and security flaws. It maintains encrypted backups to protect against data loss. It also employs a variety of user security measures. Among other things, users must use strong passwords and change them every 90 days. After 30 minutes of inactivity, users must re-establish their login credentials. An audit trail feature records user activity for full traceability.

For best results in terms of security, performance and feature compatibility, the American Red Cross and BloodHub recommend using only the latest versions of browsers and operating systems.

HIPAA and Connect®

When the American Red Cross performs blood-related services (such as blood collection, processing, distribution, crossmatching, testing, and clinical services), it is not a "business associate" of the hospitals and other customers to which it provides these services. Unless the Red Cross is performing reference testing, the Red Cross does not receive information about the patients who receive the blood the Red Cross supplies to its customers. When the Red Cross does receive patient information in connection with reference testing or clinical services (such as therapeutic apheresis, stem cell collection, or therapeutic phlebotomy), it does so for treatment purposes. Under the HIPAA Privacy Rule at 45 CFR § 160.103, a health care provider does not need a business associate agreement if it is providing patient information to another health care provider for treatment purposes. Thus, use of American Red Cross Connect does not require a business associate agreement with the Red Cross. However, the American Red Cross ensures that rigorous security measures are in place to protect patient data, as described above.