DATA SECURITY AND COMPLIANCE STATEMENT

The security and privacy of data is a core part of our business, and is our top priority. This document outlines our corporate statement regarding our data security program and the process we follow to ensure information security and compliance.

eBridge's document management system helps customers comply with the network perimeter security and data retention criteria mandated in such regulations as the Health Insurance Portability & Accountability Act (HIPAA), Gramm-Leach-Biley Act (GLBA), Sarbanes-Oxley Act (SOX), Federal Information Processing Standardization (FIPS) and the Government Information Security Reform Act (GISRA). eBridge has been certified as a HIPAA/HITECH compliant service organization, as well as a SOC2 Service Organization, by the third-party auditing firm 360 Advanced, P.A.

ENCRYPTION

Data transfer: eBridge uses Transport Layer Security (TLS 1.0 to 1.2 depending on browser and OS support) technology for mutual authentication, data encryption and data integrity. That includes the eBridge Print Driver, Web Scan and Import processes. TLS is the industry standard security protocol for encoding sensitive information. TLS creates a shared digital key, which lets only the sender and the receiver of the transmission to scramble or unscramble information.

Data storage: To ensure data security, eBridge stores all customer data AES 256 Block CBC encrypted, which meets FIPS 197 standards. This includes custom hard drive and DVD backups sent to customer locations. All files have unique keys known only to the customer. eBridge staff does not have access to the unencrypted data.

PHYSICAL REDUNDANCY

eBridge's customer data is backed up in real time to two separate data centers (Tampa, FL and Atlanta, GA). Both data centers house redundant web and database servers – fully configured with all software and data — so that in the unlikely event of a failure of any of the data centers, the backup data center will be available.

OFF-SITE BACKUPS

All eBridge customer encrypted data is also backed up at our secure off-site location each night. The eBridge backup storage location is highly secure and includes alarms, controlled access and fire suppressors — everything necessary to ensure valuable customer data is always secure.

ACCESS AND EVENT MONITORING

eBridge maintains and regularly reviews a real-time and long-term event and login access monitoring system to adhere to demands of regulatory compliance requirements like HIPAA and SOX.

PASSWORDS

Passwords are stored salted SHA512 hashed and the length and complexity can be pre-determined by your staff.

PHYSICAL SECURITY

Our data centers are managed by eBridge employees, ensuring that no outside parties gain access. The exact locations of the data centers were chosen to protect against catastrophic events and are confidential and undisclosed to protect against user data being targeted. These facilities are guarded 24 hours a day.

In addition, strong methods of entry protection such as secure token cards are used to ensure that only authorized personnel can gain access. Only select eBridge employees have access to the data center facilities and the servers contained therein, and this access is tightly controlled and audited. All data centers are also CCITV monitored with 30 days of recording backup.

DATA SECURITY AND COMPLIANCE STATEMENT

eBridge's products and services meet the physical and technical standards and provide all necessary controls for our customers to maintain their administrative security compliance. Specifically, eBridge agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic information that we create, receive, maintain, or transmit on behalf of our customers.

eBridge has implemented reasonable and appropriate safeguards to protect our customers' business information. Furthermore, eBridge agrees to report to our customers any security incident of which it becomes aware, and will authorize the termination of any customer contract in the case of any material breach of this compliance statement.