BLI Messaging and HIPAA

BLI Messaging is cognizant of the regulatory requirements the use of our services face in environments subject to compliance with the Health Information Portability and Accountability Act (HIPAA).

As it has become common knowledge throughout the medical industry, HIPAA has introduced many policies and procedures regarding the handling of patients' protected health information (PHI). However, as defined by HIPAA standards, hardware or software owned by BLI cannot be considered "HIPAA compliant". We are, though, dedicated to assisting our clients and their business partners comply with HIPAA regulations.

In summation, it is of the responsibility of medical practices (covered entities) to ensure that their patients' individually identifiable health information remains unscathed. BLI Messaging has implemented technical specifications and benchmarks to meet and exceed these regulations on our clients' behalf. Along with protecting PHI through three fundamentals: encryption, authentication and data integrity, we will never disclose any HIPAA-regulated data to anyone without probable cause and consent. The following information elicits the precautionary measures we've taken to ensure the inviolability of our clients' PHI:

Administrative Safeguards	*As Stated:*	*Implementation Specification*	*Our Solution*
Contingency Plan § 164.308 (a)(7)	"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information."	**Data Backup**	All data is backed up and stored in a secure off-site facility. Full backups of data are performed daily, with incremental backups multiple times throughout the day, allowing for point-in-time restore.
		Disaster Recovery	BLI Messaging has a full recovery plan for all aspects of our network. Monthly restore tests are conducted to ensure that all procedures are production-ready.
		Emergency Mode Operation Plan	BLI Messaging has policies and procedures in place for managing emergency situations. Our platform is geodispersed in multiple data centers, allowing for full redundancy in the event of an emergency or a disaster.
Physical Safeguards	*As Stated:*	*Implementation Specification*	*Our Solution*
Facility Access Controls § 164.310 (a)(1)	"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."	**Facility Security Plan**	BLI's secure off-site server locations require photo ID and an approved, legitimate reason for accessing the facility in which they are housed.
Workstation Security § 164.310 (c)	"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."	---	All workstations auto-lock after 15 minutes of inactivity. A second layer of authentication is required to access any client data beyond what is available from the workstation.

Technical Safeguards	*As Stated:*	*Implementation Specification*	***Our Solution***
Access Control § 164.312 (a)(1)	"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified."	**Unique User Identification**	BLI Messaging has a per-user login and password authentication for every account created.
		Emergency Access Procedure	The BLI Messaging Platform is located at redundant data centers in geographically dispersed locations, allowing for access at multiple points in the case of an emergency.
		Automatic Logoff	Each login session has an automatic logoff timeout of 30 minutes.
		Encryption and Decryption	Data moved between multiple points are secured using 128-bit SSL encryption technology and a combination of pre-shared keys and client and server certificates.
Audit Controls § 164.312 (b)	"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."	---	All access requests, reads, writes, and updates are logged by secure audit trails and monitored closely. Our non-repudiation techniques guarantee the authenticity and verifiability of these logs.
Integrity § 164.312 (c)	"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."	**Authentication Mechanism**	Health information is not maintained in the BLI Messaging platform. The platform contains transient data which is removed following the delivery of the message.

Technical Safeguards (Cont.)	*As Stated:*	*Implementation Specification*	***Our Solution***
Person or Entity Authentication § 164.312 (d)	"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."	---	BLI Messaging servers are hosted in a Tier III data center requiring keycard access to the servers. All personnel requesting access must provide photo ID and an approved reason for accessing the data. Data is encrypted and can only be accessed by authorized personnel and the end-user of the system.
Transmission Security § 164.312 (e)	"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network"	**Integrity Controls/ Encryption**	Data moved between multiple points are secured using 128-bit SSL encryption technology and a combination of pre-shared keys and client and server certificates.