Boostlingo HIPAA Compliance Matrix

HIPAA COMPLIANCE		BOOSTLINGO HIPAA COMPLIANCE	
HIPAA REQUIREMENT	**HIPAA REFERENCE**	**WHAT**	**HOW**
SECURITY INCIDENT MANAGEMENT	164.308 (a)(4)(ii)(B,C)	Tracking unauthorized access attempts in an effort to reduce risk and exposure to threats from outside network attacks and malware.	All application server infrastructure and logging data are only available via secure VPN access. Automated testing tools (IDS/IPS) are supplied by hosting environment and run on schedule. Inbound and outbound packet filtering provided by network access control lists and security groups. DDoS resilient architecture and mitigation systems automatically detect and filter excess traffic. System utilizes advanced logging and Monitoring. Access to cloud provider follows RBAC and use least privilege which can only access modules necessary for their legitimate purpose. DB infrastructure is not internet accessible. Can only be accessed by internal authorized IP's only. Application server infrastructure and logging data are only available via secure VPN access. DB infrastructure is not internet accessible. Can only be accessed by internal authorized IP's only. Access to cloud provider follows RBAC and use least privilege which can only access modules necessary for their legitimate purpose
ACCESS MANAGEMENT	164.308 (a)(4)(ii)(B,C) 164.308 (a)(5)(ii)© 164.312 (a)(2)(i) 164.312 (a)(2)(ii) 164.312 (a)(2)(iii) 164.312 (c)(1,2)	Information is only decrypted for authorized access users only	256 AES Encryption in transit and at Rest. All requests to/from our servers are made over encrypted https (TLS 1.2) using only the most secure cipher suites. Our database instance, and all of its backups, are encrypted at the volume level.
ENCRYPTION and DECRYPTION	164.312 (a)(2)(iv) 164.312 (e)(2)(i) 164.312 (e)(2)(ii) 164.312 (c)(2)	File and Application Level encryption	256 AES Encryption in transit and at Rest. Boostlingo uses a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to host, maintain and deploy the solution across all platforms. Boostlingo infrastructure is a multitenant public cloud solution with the ability to segregate data by tenant on their own dedicated instance. All User information is encrypted in the Boostlingo DB.
KEY MANAGEMENT	164.312 (e)(2)(i)	Key management via secure web management system	Utilize IAM roles to change access keys and revoke credentials. Keys and passphrases are only readable by the system root user. The access keys are securely stored in a key management service provided by our cloud host provider. This is required to startup the instances since we use volume level encryption. Only the necessary development/operations members at BoostLingo, have access to this key service. The key management service we utilize takes advantage of Hardware Security Modules to protect the security of the keys. The service is built on systems that are designed to protect the master keys with extensive hardening techniques such as never storing plaintext master keys on disk, not persisting them in memory, and limiting which systems can access hosts that use keys.

LOGGING AND AUDIT CONTROLS	164.312 (b)	Data Event logs generated daily and maintained	HTTPS is the only form of communication allowed to the BoostLingo API. The SSL certificate can (and should) be validated in the client's web browser. Mobile apps also consume the same API and will prevent access if the certificate does not match or is no longer valid.Boostlingo captures the following: • Server reboot/shutdown/start up events • Software package and update events • System administrator logins and login attempts • Device failure and hardware error codes • Application logs include: o Call completion o Service interruptions o Device heartbeato Call errors Customers do not have direct access to their own system logs, but can be supplied to them upon request to Boostlingo. All user login failures are logged. All security incidents are escalated to senior technical staff and when found to be true threats are logged against internal ticketing system for mitigation.
MONITORING	164.308 (a)(1)(ii)(D)	Monitoring access to PHI	Boostlingo monitors all servers and network hardware the application is running on. Internal and external monitoring checks all of the monitored devices at 5 second intervals. Roles Based Management can be used to restrict access to those users who should not have access to PHI information. All user activity is logged.
SECURITY INCIDENT MANAGEMENT	164.308 (a)(1)(ii)	Identify incidents if they occur to quickly remedy	Security incidents are communicated to administrators through email/text/phone call and require recognition to close incident or same notifications remains open and hits additional administrators. All security incidents are logged in the security incident register. Security incidents, when and if detected, are handled at the highest priority by working with the Hosting environment. All data is encrypted, hashed and salted. All security incidents are escalated to senior technical staff and when found to be true threats are logged against internal ticketing system for mitigation.