Backline

HIPAA COMPLIANCE CHART

Backline Ensures HIPAA Compliance

DrFirst's secure messaging platform, Backline, allows your institution the convenience of messaging while remaining in compliance with the relevant HIPAA standards. In fact, we have put together a simple chart that lays out this information below.

HIPAA Standard Standard Number Implementation Specification	Backline Capability
Access Control 164.312(a)(1) (i) Unique User Identification (iii) Automatic Logoff	Backline uses unique username and password to authenticate with the messaging server. Backline for iPhone and Android can be set up to require a four-digit PIN to access by the administrator. An inactivity setting automatically times out sessions on Android, iPhone, or Web and Admin Console.
Access Control 164.312(a)(2) (iv) Encryption	**Backline messages:** All data is encrypted within Backline's storage and in communications between nodes. **Backline for iPhone and Android:** Conversations and proprietary data for each hospital is encrypted on every mobile device using AES-256, protected with the user's PIN. **Backline for Web:** No permanent data is stored in web browser, and non-caching directives are used.
Transmission Security 164.312(e)(1)	All data in transit is secured with TLS AES-256 and RSA 2048. No PHI is exchanged with web services, and all credentials and invitation codes are also encrypted using TLS.
Person or Entity Authentication 164.312(d)	A user is first provisioned with an invitation code from an administrator, which expires in seven days. Credentials generated during sign-up are stored on the mobile device for subsequent authentication when the user provides a four-digit PIN. Credentials on devices are protected using AES-256 encryption.

HIPAA Standard Standard Number Implementation Specification	Backline Capability
Audit Controls 164.312(b)	Product automatically logs the following: • All administrator activities related to managing users and policies • All authentication events • Time-stamped message delivery and read receipts
Workforce Security 164.308(a)(3)(ii) (C) Termination Procedures	Administrators can disable users using the Backline Admi Center or by disabling the user Active Directory. Once disabled users cannot access the directory or any messages belonging to that hospital stored on the mobile device.
Security Awareness and Training 164.308(a)(5)(i) (A) Login Monitoring (B) Password Management	Backline restricts access to the application until the correct PIN is entered. Web users can change their passwords or request a password reset using an invitation code issued by the administrator. Should a user fail to enter the correct password 3-5 times they will be locked out for 15 minutes on all devices.

Corporate Headquarters
9420 Key West Ave., Suite 101
Rockville, MD 20850
Toll Free (866) 263-6511

West Coast Office
1640 South Stapley Drive, Suite 122
Mesa, AZ 85204
(602) 466-7547

sales@drfirst.com | www.drfirst.com | blog.drfirst.com

DrFirst

© 2017 DrFirst Corporation. All rights reserved.