Security Notice

How We Protect Your Data on Our Web-based Software Services

What This Security Notice Covers

This security notice pertains to the security measures in place at Beats Health for protection of personal and protected health information in connection with the use of the Beats Health web site, Beats Health Patient Eligibility Verification, Beats Health Referral, Beats Health Authorization, Beats Health Patient Cost Estimator, and related services under this agreement (e.g., Beats Health Dashboard) **(Service)**.

Unique identification of users

To comply with the HIPAA requirements and to provide a secure service, Beats Health requires all users to have a unique login credentials. Beats Health currently requires a valid email address to be the username for the Beats Health Products and Service.

In addition to a username, every user account must be protected with a password of sufficient complexity. Beats Health requires its customers to meet password complexity requirements as indicated in the Product website. If your user account has access to multiple Beats Health customers, you will be required to use the more restrictive policy.

All Beats Health Service sign-ins are protected by account lock-out systems. If a user incorrectly authenticates a number of times or the user's account is locked by a system administrator, their user account will be locked until a system administrator of the user 's account unlocks it. Beats Health's support team is prohibited from unlocking user accounts unless the account is the system administrator account.

Security on the Beats Health web site

Beats Health Service users may choose to sign into their account at the Beats Health web site in order to access the downloads or account status. Such sign-ins are protected by SSL security. Your browser will usually display an indicator (such as a "lock" icon) when using a secure SSL connection.

Security in the Beats Health service

The Beats Health Service communicates with secure Beats Health hosted and controlled servers and networks. All communications are secured with public-key encryption. Beats Health disallows the use of low cipher strength in our production service.

Beats Health helps to ensure protection of customer and patient data, as it encrypts data and stores data in access-controlled cloud servers.

In addition to these controls, Beats Health deploys up to date advanced threat protection services which help to identify, block, and track hacking attempts, scans, data breaches, adware, malware, spyware, Trojans, phishing attempts and other equally malicious requests.

Role-based security

Every user in the Beats Health Service belongs to one or more roles. A role is defined by each customer and is assigned a set of permissions. Beats Health roles follow an allow-then-deny pattern of applying permissions — such that multiple role permissions are combined, and then filtered against any role's restrictions.

Application locking

In accordance with HIPAA policies, Beats Health's Service will automatically logout if left unattended for a period of time. Users need to login to use the application again.

Beats Health password policy

Beats Health system passwords are meant to help protect sensitive patient medical and financial records, as well as practice financial information. They serve as a deterrent to malicious agents as well as protection against casual or accidental lowering of security through carelessness.

The passwords are encouraged to be at least (8) eight characters long and have to maintain a level of complexity such that they will not be easily guessed or cracked by a determined attacker.

A user may change their password at any point in the application. Passwords changed by third parties will immediately expire to allow users to log in but also to ensure that they immediately change their passwords to something that only they know.

Beats Health will never store any passwords in permanent storage in a way that is reversible. The Beats Health Service will never show the password in plain-text, human-readable form.

Changes to this security policy

Beats Health may update this policy at any time for any reason. If there are any significant changes to how we handle security, we will make a reasonable commercial effort to send a notice to the contact email address specified in your company's Beats Health account or by placing a prominent notice on our site.

Questions?

If you have questions or suggestions, you can contact us at:
info@thebeatshealth.com

Last Updated: This policy was last updated on August 5, 2021