

Automated Medical Assistant (AMA)

Security Notice

What this security policy covers

This security policy pertains to the security measures in place at Advanced Billing Solutions, Inc. (ABS) for protection of personal and protected health information.

Unique identification of users

To comply with the HIPAA requirements and to provide a high quality secure service, Advanced Billing Solutions, Inc. (ABS) requires all users to have a unique username. Advanced Billing Solutions, Inc. (ABS) currently requires a valid email address in addition to a unique username in order to access the Automated Medical Assistant (AMA) service.

In addition to a username, every user account must be protected with a password of sufficient complexity. Advanced Billing Solutions, Inc. (ABS) allows its customers to set their own password complexity policy

All Advanced Billing Solutions, Inc. (ABS) sign-ins are protected by account lock-out systems. If a user incorrectly authenticates a number of times, their user account will be locked until an administrative user unlocks it.

Security on the Automated Medical Assistant (AMA) web site

Access to the Automated Medical Assistant (AMA) service is protected by SSL security. Your browser will usually display an indicator (such as a "lock" icon) when using a secure SSL connection. The service/application is located on a server hosted entirely by Advanced Billing Solutions, Inc. (ABS). All communications are secured with public-key encryption.

Group-based security

Every user in the Advanced Billing Solutions, Inc. (ABS) system belongs to one or more groups. Group assignments are defined by the Administrator of each practice. Each group dictates a set of permissions.

Application locking

In accordance with HIPAA policies, the Automated Medical Assistant (AMA) service will automatically lock up if left unattended for a period of time. Correct credentials of the user will need to be provided prior to using the application again.

Advanced Billing Solutions, Inc. (ABS) password policy

Advanced Billing Solutions, Inc. (ABS) system passwords are meant to serve as the last line of defense in protecting 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 as long as possible and 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 time on the login screen.

Advanced Billing Solutions, Inc. (ABS) will never store any passwords in permanent storage in a way that is reversible. The Automated Medical Assistant (AMA) software will never show the password in plain-text, human-readable form.

Changes to this security policy

Advanced Billing Solutions, Inc. (ABS) may update this policy at any time for any reason. If there are any significant changes to how we handle security we will send a notice to the contact email address specified in your company's Advanced Billing Solutions, Inc. (ABS) account or by placing a prominent notice on our site.

Questions

If you have questions or suggestions you can contact us at:

Advanced Billing Solutions, Inc. (ABS) Security Administrator
150 S.W. 12th Avenue, Suite 330
Pompano Beach, FL 33069
AdvancedSolns@aol.com

To report a security violation, please call us at 800-815-BILL.

Last Updated

This policy was last updated on February 28, 2009.