HIPAA Compliance Security Overview

A Secure Platform for Patient Engagement

The Health Insurance Portability and Accountability Act, or HIPAA, is a federal law that requires special handling of personal health information (PHI). Utila was developed from the ground up with HIPAA compliance in mind by security experts, legal consultants, and mental health professionals. In accordance with HIPAA, Utila has physical, technical, and administrative safeguards to ensure that data transmitted through Utila is kept totally secure.

TECHNICAL SECURITY FEATURES

Utila meets and exceeds the technical requirements set forth by HIPAA.

- All users have unique login credentials
- All user activity creates an audit trail
- Data is encrypted in transit and at rest
- Users create security questions for password recovery
- Users are automatically logged out if the application idles
- Passwords are salted to protect against hackers
- Database has multi tenant structure for additional protection to organizations

ADMINISTRATIVE SAFEGUARDS

Utila has comprehensive policies and procedures to ensure that users' data is kept safe and secure. Utila's developers are trained in HIPAA compliance standards as well as Utila's internal policies and procedures. Utila enters into a Business Associate Agreement with its providers, whereby Utila agrees to safeguard personal health information (PHI) and report security breaches as required by HIPAA.

PHYSICAL SAFEGUARDS

Utila's application and data are hosted on Google Cloud's HIPAA compliant infrastructure.

This statement was updated December, 2015. For more information visit www.utila.us, or contact Utila's Privacy Officer, J. Zach Boone, MSW, at zach@utila.us

WE SUPPORT YOUR ORGANIZATION

As a part of the onboarding process with each organization, we provide training and ongoing support to organizational administrators and providers. Our goal is for you and your users to have an understanding of how to use the Utila product in a safe and secure way.

Responsibilities of all users:
We try to make our product as intuitive and easy to use as possible. However, all users must have a basic familiarity with web-based software, SMS text, and email and may require some basic training to safely use the Utila application. All users should use a strong password with a mix of both capital and lower case letters, numbers, and special characters (like '#', '@', or '$') when creating accounts with Utila. Users should periodically change their passwords, and should not use passwords used for other accounts. Users should not share their login credentials with anyone. Although we automatically log users out if the application idles, users should be in the habit of always signing out and closing their browser tab when they are finished using Utila. Users should also be sure to install software updates as soon as they are available in order to protect devices from the latest security threats. Because Utila is web-based software, there is no need to install anything to use Utila. However, users should use an updated web browser like Google Chrome.

Responsibilities of organization administrators:
Organizational administrators are responsible for managing provider accounts. Organizational administrators should only activate accounts for providers that have received the initial training and orientation to the Utila product. Organizational administrators are responsible for revoking permissions of providers as appropriate (for example if a provider no longer works for the organization).

Responsibilities of provider users:
It is the provider's responsibility to provide an initial orientation to clients regarding the Utila product and obtain clients' informed consent. Although we do our best to provide an intuitive user experience, providers should explain to clients how Utila can benefit them and what the potential risks are.

MULTIPLE CHANNELS OF COMMUNICATION

The Utila product currently supports three different modes of client engagement.
In-app: users are required to login to the Utila application in order to access information. This is the most secure mode of communication.
Email and SMS: providers can deliver reminders, check in messages, and educational resources by email and/or SMS. Because email and SMS are inherently less secure than transmitting data inside the Utila application, providers and clients should include only information that they are comfortable receiving via SMS or email. We allow organizations, providers, and clients to configure messages to contain only information that your users are comfortable receiving via SMS text and email. We help you configure messages as a part of the onboarding process.
Opt out: clients can opt out of SMS text by responding 'Stop' at any time. Client's can also update their preferences and delete their accounts by logging into the Utila application.

UTILA ARCHITECTURE