Security Overview

Last Updated Oct 3, 2018

Table of Contents

- Introduction
- Schedule Data
  - Overview
  - What is contained in my Amion schedule?
  - Where is my schedule stored?
  - Is my schedule encrypted?
  - How does schedule data move through Amion?
  - Are my schedules backed up?
  - How long are schedules kept on Amion?
  - What happens to my data if I don't renew my account?
  - How reliable is Amion?
  - Does Amion require a unique username and password for every user?
  - Are complex passwords required?
  - Does Amion provide role-based security?
- Message Data
  - Overview
  - How does message data move through Amion?
  - Traditional pagers and SMS text messages
  - Third Party Secure Messaging Services
  - Amion Secure Texts
    - How does the Doximity verify identities?
    - Is Amion App text messaging HIPAA compliant?
    - What kind of safety measures / encryption are provided in the Amion App?
    - If I lose my device, can anyone else access my messages?
    - Where are messages stored?
    - How long are messages retained on the server?
    - Can Amion or Doximity read my messages?
    - Where can I find more information about Doximity's security and HIPAA compliance?
  - Which messaging option is right for my schedule?
- Additional Security Options
  - Schedule Level Options
  - Enterprise Level Options
  - Active Directory Integration

Introduction

Amion is a tool that helps build, publish, and share physician and medical provider schedules for individual groups, whole hospitals, or entire hospital systems. Amion also assists with communication by integrating with a variety of messaging and paging options and includes its own first party secure messaging system as an option.

Amion handles two types of data: schedule data and messages. We handle these types of data separately and with different approaches to security. This document explains Amion's practices with regards to both schedule data and messages.

Schedule Data

Overview

Amion schedules are easy to access from anywhere. Since Amion schedules don't contain any patient data or PHI (Protected Health Information) and aren't covered by regulations like HIPAA we are able to prioritize ease-of-use over security while still ensuring that Amion schedules are generally visible only to those who need to see them.

Amion schedules are created by a scheduler using OnCall, Amion's desktop schedule building software. The scheduler then posts them to Amion using their **Admin password** (set when creating the account.) The staff view the schedule online (read-only) at amion.com using a shared **Staff password**. Administrators don't need to create separate accounts for each person who views the schedule, they can simply share the staff password with them.

This describes a typical Amion implementation. There are additional security options you may enable, such as Active Directory integration, described later in this document.

What is contained in my Amion schedule?

An Amion schedule does not contain any PHI. Although schedules vary, most Amion schedules contain only the following:

- Service/Call/Shift names
- Staff names (Names may be in any format. Initials or other less-identifiable substitutes may be used.)
- Schedule Assignments
- Staff contact information (Optional, with a variety of settings for visibility)
- Administrator email address

Where is my schedule stored?

Schedule data is stored on the computer on which it is created (while being edited, and as a backup) and on the Amion server. Amion is a hosted application running on a Linux server with an entirely custom codebase. Amion does not rely on any third party database or other dependencies that may introduce bugs or security vulnerabilities. Each schedule is stored in a separate file and directory. Schedules are created and stored in Amion's .sch file format.

Amion's server is hosted by MIVA Merchant from their data center in Tampa, FL. Only Amion has access to the servers' contents. MIVA is a PCI Certified enterprise hosting provider.
Information about MIVA's PCI Compliance
Attestation of Validation

Is my schedule encrypted?

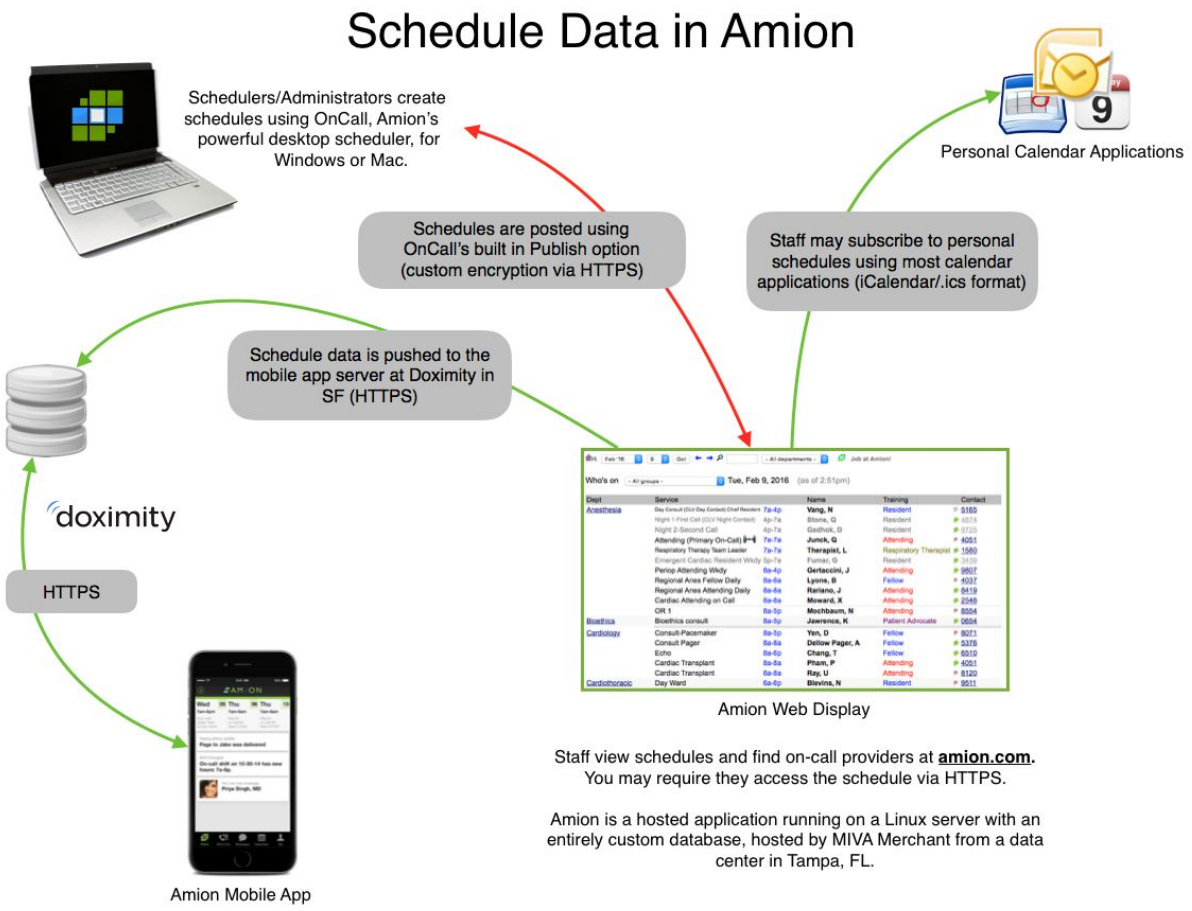
You may require that schedules be accessed via HTTPS (encrypted in transit.) Amion currently supports all TLS versions. For security reasons, our hosting provider MIVA intends to disable TLS 1.0 and 1.1 by June 30th, 2018.

OnCall and Amion share an algorithm for generating a custom 128-bit encryption key each time the schedule file passes from the client to the server or vice versa. The key does not travel with the data but each side knows how to generate the key and decrypt the file.

Amion schedules are not stored encrypted at rest on the Amion server or on the administrator's workstation. Personally identifiable information within the schedule may optionally be encrypted at-rest on Amion's servers for Enterprise Account customers. When not encrypted, the schedule files contain a mix of text and binary data. The text would be shift names, staff names and contact info, and sticky notes schedule admins attach to shifts. No patient data and no text messages travel with the schedule.

How does schedule data move through Amion?

See our flow diagram below:



Are my schedules backed up?

Yes. Amion keeps several types of backups, including complete offline backups. In case of accidental deletions or other issues, administrators may access online backups of their Amion schedule going back 28 days.

How long are schedules kept on Amion?

Indefinitely. We will remove old schedules at the request of the administrator, but generally schedules remain accessible on Amion as a record until they are removed or replaced by the administrator.

What happens to my data if I don't renew my account?

For expired accounts, no new data can be published but old schedules are maintained indefinitely until you choose to remove them.

How reliable is Amion?

Amion has exceptional uptime of over 99%. All web updates happen transparently with no down time and with subtle or minimal visual or functional differences from one revision to the next.

Does Amion require a unique username and password for every user?

Amion has many options for allowing access, ranging from a simple shared login for read only access to requiring individual Active Directory logins per user.

You designate which staff have access to building/updating schedules. Each schedule/group has its own administrator password (shared by the administrators) that allows read-write access to the schedule. Amion records if a change is made by a switchboard operator login, an administrator web login, or an administrator using OnCall (Amion's desktop schedule building software), and displays the workstation ID or username from which the schedule was last published, but does not distinguish between individual administrators of a single departmental schedule.

You define which staff/providers can view schedules online at Amion through a view-only password (shared by the staff in that group.) Amion does not log individual viewers of the schedule. Individual groups may have their own passwords, or you may designate a site-wide view-only password, or both.

Staff/providers can submit requests (vacation, availability, swaps, etc...) via a private password which they set up via an email login. This password can be changed by the user.

In Enterprise accounts, the Enterprise administrator has access to all schedules and to adding schedules, emailing schedulers, and accessing/editing account information.

Intranet links or desktop shortcuts can be created to allow password-free access to the schedule.

Enterprise accounts have the option of using Active Directory integration to require individual staff logins to view the schedule page. Active Directory integration is further explained in the *Additional Security Options* section of this document.

Some additional options are available. See the Additional Security Options section for more details about allowing and limiting access to schedules.

Are complex passwords required?

Our only requirement is that passwords be unique. Passwords may be managed centrally by the enterprise administrator who can enforce stricter requirements if they wish. If Active Directlry integration is used, your existing Active Directory passwords and password policies apply.

Does Amion provide role-based security?

Yes, access to Amion schedules falls into four categories: Staff, Switchboard, Administrator, or Enterprise Administrator. Staff can be separated by “Training” or “Staff Type” for convenience when scheduling but all staff have read-only access to the schedule.

Message Data

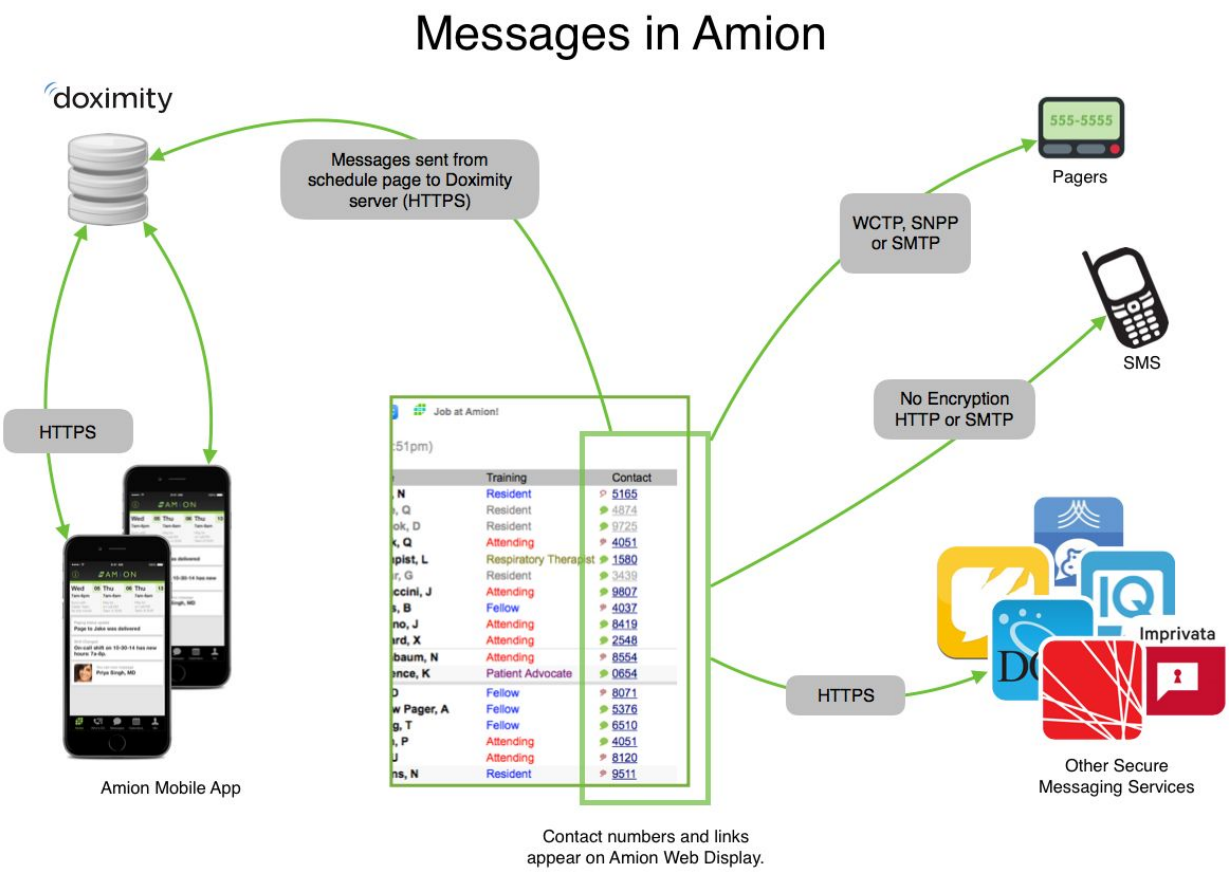
Overview

For many years Amion has integrated with traditional pagers and SMS text messaging, allowing staff viewing a schedule online to send a message to an on call provider with one click. As groups have begun to replace or supplement their pagers with HIPAA compliant secure messaging apps and services, Amion has adjusted our approach to meet these requirements by integrating with many existing services, and by offering our own HIPAA compliant messaging app.

Amion integrates with numerous types of messaging services, some of which are encrypted and HIPAA compliant and some of which are not. Which of these you implement on your schedule (if any) is up to you.

How does message data move through Amion?

See our flow diagram below:



Analog pagers and SMS text messages

If a schedule is configured to enable traditional pagers or SMS text messages, staff phone or pager numbers listed on the schedule will be clickable hyperlinks that connect to a form for sending a message. Messages are one-way, and are handed off from the Amion server to the messaging provider in the fastest and most reliable way they support. This may include WCTP, SNPP, SMTP, or HTTP.

Typically anyone with access to view the schedule may send a page, but you can require a personal password (such as the ones used when submitting time-away requests) for additional security. Because no SMS or pager messages are encrypted these messages should not be considered HIPPA compliant and should not contain PHI.

Third Party Secure Messaging Services

Amion integrates with a number of third party secure messaging services including (but not limited to) *TigerConnect*, *Cortext*, *DocHalo*, and *Everbridge*. In these cases we deliver messages using the programming/messaging interface provided by those messaging services. Amion acts only as a conduit for messages sent from the Amion schedule page. Messages are one way, and are encrypted in transit between us and the messaging provider.

Staff configured in Amion to receive third party secure messages will appear on the Amion schedule page with a secure message icon next to their name. This may be instead of or in addition to any other contact information. Clicking that icon will connect to a form for sending a message.

Typically, as with SMS text messages, anyone with access to view the schedule may send a message. You may require a personal password (such as the ones used when submitting time-away requests) for additional security. These messages employ the same security as other messages through the messaging provider.

If you aren't sure if your existing messaging provider allows integration with Amion, reach out to us at support@amion.com.

Amion Secure Texts

Amion has partnered with Doximity to provide HIPAA-compliant secure texting for all Amion schedules via our mobile app.

Staff may install the Amion mobile app on any iPhone or Android smartphone. The app is available as a free download from the iPhone App Store and the Google Play store. (Windows Phone and Blackberry are currently not supported for secure messaging though they may receive traditional unencrypted text messages.)

After installing the the app the physician or staff member verifies the their identity using a Doximity account. Doximity is the leading medical professional network with half of U.S. physicians as members, and they have partnered with Amion in creation of the mobile app and messaging. If your staff don't already have a Doximity account they may create one in the app for free.

How does the Doximity verify identities?

Doximity uses a number of sources to verify physician identity, including but not limited to faxed copies of medical credentials and emails from officially recognized medical institutions (school or hospital). In most cases, they may register an account and verify their identity without leaving the app.

Is Amion App text messaging HIPAA compliant?

Yes, Amion text messaging is HIPAA compliant because all messages are encrypted via the secure Doximity messaging API. Any messages you send through the app are protected with a code to prevent outside parties from reading them.

What kind of safety measures / encryption are provided in the Amion App?

Highlights of the Amion App/Doximity's security and compliance components include:

- Unique user identification and verification
- User authentication to confirm the medical professional's identity
- SSL handshake protocol with 2048bit RSA cryptosystem
- Secure inbox with end-to-end 256bit AES digital encryption with CBC mode
- Audit control to protect users from security violations
- Backup of all network activity

If I lose my device, can anyone else access my messages?

No one else can access your Amion messages if you lose your device. The Amion mobile application for iOS and Android does not store PHI locally on mobile devices. Rather the data transmitted to mobile devices is erased from the device after access, while the version on Doximity servers remains encrypted at rest. In the event a user has a lost or stolen mobile device, the user or Amion support can deauthenticate the device remotely. In the event that you have a lost or stolen mobile device, you can deauthenticate the device or contact support@doximity.com.

Where are messages stored?

Amion secure messages are stored on a Doximity messaging server hosted from their hosting facilities in San Francisco.

In Amion enterprise accounts, messages sent via the Amion schedule page are also logged on the Amion server so that staff with Switchboard access can view a record of recently sent messages. This feature can be disabled if you wish.

How long are messages retained on the server?

Currently, messages are retained indefinitely. (This is subject to change.)

Can Amion or Doximity read my messages?

No. Messages are encrypted-at-rest on the Doximity server.

Where can I find more information about Doximity's security and HIPPA compliance?

Doximity provides the following documentation:

- Whitepaper: Amion & Doximity (PDF)
- Whitepaper: HIPAA & Doximity (PDF)
- Doximity Privacy Policy and End User License Agreement

Which messaging option is right for my schedule?

You may use multiple different types of messaging within a single schedule. Below is a comparison of Amion's messaging options:

	Traditional SMS/Paging	Third Party Secure Messaging (ie TigerConnect)	Amion Secure Texts
Send from schedule page	Yes	Yes	Yes
HIPAA Compliant (Can include PHI)	No	Yes	Yes
Integrated with Amion mobile app	No	No	Yes
Delivery Confirmation & Read/Unread Status	No	Yes	Yes
Cost	n/a	Varies, charged per user.	Included with Amion scheduling for any number of users
Attachments*	Photos only	Yes	Photos only

Advanced reporting for administrators	No	Yes	No

* Messages sent from the Amion.com page may not include attachments. Attachments may be added when sending via a mobile device

Additional Security Options

Amion offers a number of ways to customize the security and accessibility of various parts of a schedule. The following is a non-exhaustive list of options that may be enabled to customize the security of your schedule.

Schedule Level Options

Schedule-level options can generally be set by the administrator of a single group or departmental Amion schedule.

- Most individual schedule features may be disabled
    - This includes hiding contact info, disabling messaging, hiding shift times, and numerous other small customizations
- Hide vacations/off schedule services from staff
- Limit staff to viewing “Who’s On” lists unless they have secondary or personal password
- Require a personal password to login & reject it past their quit date
- Disable the ability to send Amion secure messages from schedule page
- Allow messaging but hide contact info, showing only a generic pager or message icon
- Require a personal password to send messages
- Passwordless link directly to schedule from intranet page
    - Some groups restrict access by linking directly to their Amion schedule page from a hospital intranet site, and not sharing a login with staff so that it can only be reached from that link.

Enterprise Level Options

- Require SSL/HTTPS when accessing the schedule page
- Require both site & group passwords to access schedules
- Require both site and personal passwords to access schedules
- Disable the ability to send Amion secure messages from schedule page (site-wide)
- Enable or disable message logging
    - Amion logs pages and messages sent via the schedule page to enable staff with Switchboard access to see a log of recent pages. You may disable this.
- Show or hide contact info

- Show hidden contact info only to staff with Switchboard access
- Passwordless link directly to Enterprise Who's On list from intranet page
- Enable at-rest encryption of personally identifiable information
- Host a local Amion server
    - As an option for groups who require a locally hosted service rather than an online service, enterprise accounts may use their own hardware to host a local instance of the Amion server for $1000 per year. This option is unnecessary for most groups.

Active Directory Integration

In early 2016 Amion added support for Single Sign On (SSO) Active Directory validation via a SAML server. This feature is currently being implemented on pilot accounts (as of May 2016) and should be available as an optional add-on for every Amion Enterprise account in the near future.

If you would like to help pilot implementing Active Directory integration before it is released as an option to all customers, contact us at support@amion.com. When this feature is fully rolled out we expect to treat it as an optional extra similar to the locally hosted Amion server option, and priced at $1000 per year.