Amwell Support & Hosting Operations Guide

Amwell Platform

Document Version: 1.4 All Applications

Contents

Introduction 3
Scope and Purpose 3
Document Change Control 3
Description of Services 4
Cloud Service Providers 4
Backup Services 4
Disaster Recovery 4
System Monitoring and Alerting 4
Hosting Operations Audits 5
Service Level Commitment 5
System Availability 5
Definitions 5
System Maintenance & Continuous Delivery 5
Version Support 6
Service Level Exclusions 6
Hosting Security Practices 6
Physical Security 6
System Security 7
Network Security 7
Security Incident Reporting 7
Software Maintenance and Support 8
Definitions 8
Level 1 Support 8
Level 2 Support 9
Level 3 Support 9
Maintenance Responsibility 10
Support Responsibility 10
Error Classification, Reporting and Response 11
Documentation 12
Customer Error Reporting Guidelines 12

Introduction

Scope and Purpose

The purpose of the Amwell Support & Hosting Operations Guide is to define the processes and rules that Amwell follows in order to effectively manage hosting, support and maintenance service for its customers. This guide includes information about Amwell's scope of hosting services, service level commitments, escalation procedures, and other support obligations. It is intended to provide guidance for the Amwell operations and support teams, and information for customers' technical operations teams.

The primary objectives of this guideline are:

- Establish practices that govern the delivery of hosting, support, and maintenance services.
- Promote the security of information stored within Amwell's cloud-based Applications.
- Promote compliance with all local, state, and federal statutes related to information protection.

Document Change Control

Revisions to the Amwell Support & Hosting Operations Guide are subject to document change control. Changes to this document made be made at any time and must be approved by the Amwell Chief Information Officer. Notification will be made to customers with 30 calendar days of any material change to the Guide.

Date	Version	Comments
March, 2022	1.0	Initial version for Converge
May, 2022	1.1	Added clarification for SilverCloud Application
October, 2023	1.2	Updated terminology for Amwell Home and Hospital Applications; clarified scope of Service Level Exclusions; added Customer assisted L1 description; updated Error escalation procedure.
July, 2024	1.3	Updated Error escalation procedure; updated "platform" and "Application" terminology to align with Converge Product Schedule definitions; added clarification for Automated Care Application, clarifying definition of Documentation.
April 20, 2026	1.4	Updated document based on the removal Armor Defense, GCP clarification, AWS global cloud service provider, and removal of Auth0

Description of Services

Cloud Service Providers

Amwell delivers its platform leveraging cloud service providers located in the United States which are SOC2 Type 2 certified or certified under another equivalent standard. Amwell services are delivered from one or more of the following locations:

- Andover, MA
- Santa Clara, CA
- Amazon Web Services (AWS)
- Google Cloud (GCP)

In no event shall such hosting sites for US customers be located outside the United States.

Amwell will provide instances of its system, as follows:

- 1 dedicated instance on a multitenant production platform for cloud-based Applications
- 1 dedicated instance for customers using Amwell's Home and Hospital Applications
- Additional instances may be available under separate statements of work

Backup Services

Amwell's cloud-based Applications are hosted in Amazon Web Services (AWS) and Google Cloud Platform (GCP) facilities and leverage a combination of backup and replication strategies for continuous availability.

For Amwell's Home Application, data is backed up locally throughout the day with backups being pushed to a remote co-location data center at least once per day. Backups are also stored using secure cloud backup service providers such as Commvault. These backups are refreshed at least daily.

Backup data is maintained in accordance with our Data Handling and Information Security policies.

Disaster Recovery

Amwell's Disaster Recovery Plan (DRP) shall be used in the event of a significant disruption to the services Amwell provides to its customers. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

System Monitoring and Alerting

Amwell maintains multiple system monitoring and alerting systems which are deployed in multiple regions to detect and notify our operations teams about resource utilization, component and system

failures, and other potentially service impacting events. Alerts are monitored 24x7x365 by our Cyber Command Center (C^3).

Hosting Operations Audits

Amwell conducts internal and external audits relating to the hosting services on a regular basis. These audits are based on standards such as ISO 27001, HITRUST CSF, HIPAA, PCI DSS and/or other applicable standards. The content and format of these audits may be changed at the discretion of Amwell.

Service Level Commitment

System Availability

Amwell provides a System Availability target of least 99.90% during each calendar month, calculated by dividing Uptime Hours by the Base Hours and multiplying the result by 100. These calculations are made on a calendar month basis with service availability measured to the hundredth of an hour and hundredth of a percent of system availability (e.g., 719.*50* Uptime Hours or 99.*93*% availability).

Definitions

For purposes of this calculation, Amwell uses the following definitions.

Base Hours

"Base Hours" are the total number of hours during a calendar month.

Downtime

"Downtime" occurs when some or all major functions of the Amwell System are inoperable or inaccessible. Downtime does not include periods of scheduled or emergency maintenance, single periods lasting less than 10 minutes, or periods of inoperability or inaccessibility to the extent caused by one of the defined Service Level Exclusions. For the purpose of calculating System Availability, downtime begins the moment a Severity 1 Error is reported to Amwell.

Uptime Hours

"Uptime Hours" are determined by subtracting the total Downtime from the Base Hours.

System Maintenance & Continuous Delivery

Amwell's cloud-based Applications employ continuous integration and delivery methodology where system updates will be deployed in a rolling fashion, in most cases, without system downtime. These updates may include, but are not limited to, software, configuration and infrastructure updates. These changes are deployed via automated delivery pipelines which are supported by strict quality controls,

system monitoring, and rollback procedures. In rare cases, if a maintenance window is required for Amwell's cloud-based Applications the Customer Success team will notify the customer's designated contacts with advance notification of all scheduled, service impacting maintenance.

Version Support

Amwell's cloud-based Applications do not support previous versions of the software as these are multi-tenant environments. All version updates to Amwell's cloud-based Applications will be scheduled, deployed and managed at the discretion of Amwell. Any errors related to a version update will be investigated and managed by Amwell in accordance with the error classification definitions below.

Amwell's Home and Hospital Applications are dedicated installations, and as such, can receive support for the two previous minor releases of the software. Home and Hospital customers will receive support for any version which is two-point releases from current (If Home or Hospital Application version 12.7 is GA, Amwell will support up to 12.5 of the software).

Service Level Exclusions

Events or factors outside of Amwell's control may impact Amwell's ability to achieve the target System Availability. Amwell shall not be responsible for any failure to meet the service level commitments set forth above if the failure is due to one or more of the following (collectively, "Service Level Exclusions"):

- A customer's acts or omissions, including any customer misuse or abuse of the Applications or use in violation of the customer agreement or terms of use.
- Viruses, malware, or malicious code (given Amwell has applied generally available and approved security definitions as soon as is practicable).
- Violations of the Terms of Use or malicious attacks on the Applications.
- Any cause beyond the reasonable control of Amwell, so long as Amwell takes prompt measures to address such causes and notifies Customer thereof, including system outages of third party service providers that host or provide services to Amwell's Applications (including but not limited to: Amazon Web Services, Google Cloud, Surescripts, Contentful, Change Healthcare, Stripe, Twilio, etc., as applicable).

Hosting Security Practices

Amwell maintains a comprehensive Information Security program to protect the systems and information under its control. This program includes protections in the following areas.

Physical Security

Physical access to Amwell's facilities and those of its Cloud Service Providers is restricted to authorized personnel only with appropriate levels of logging, audit and access control applied.

Details on physical security and access for AWS-US can be found here: https://aws.amazon.com/compliance/data-center/controls/.

Details on physical security and access for GCP-US can be found here: https://www.google.com/about/datacenters/data-security/

System Security

All remote administrative access to the systems supporting the Amwell Applications requires authentication. Authentication is implemented using a minimum of username and password verification, and where required, two factor authentication. Amwell policies require that passwords must be sufficiently complex to reduce the effectiveness of "dictionary attacks" to crack these passwords. All system access is granted on a minimum necessary basis and is regularly reviewed and removed as needed. Additional controls, such as IP address restriction, proxy servers and intrusion prevention rules are configured by Amwell to prevent intruders from gaining access to the system.

Amwell will track and implement applicable security patches and updates to all software products used in the Applications, including but not limited to operating systems, database management systems, third party products, firewalls, anti-virus software, anti-virus signature/definition files, intrusion prevention and detection software or firmware used in networking equipment. Unless otherwise required, these changes shall be applied during scheduled maintenance or in a non-intrusive fashion.

No third party may have access to customer Protected Health Information (PHI) or Personally Identifiable Information (PII) without proper consent. Amwell's obligations regarding use, access to and transmission of PHI is set forth in the Business Associate Agreement between Amwell and the third party.

Network Security

Amwell leverages security devices including firewalls, WAFs and API gateways to permit only the protocols necessary to allow Amwell's Applications to function. All unnecessary protocols are explicitly denied. Monitoring and logging the security devices are designed to inform Amwell of unauthorized access or otherwise suspicious attempts to gain access to secured portions of the system across the network.

Security Incident Reporting

Amwell will use commercially reasonable efforts to investigate, respond to and terminate any security breaches or compromises.

Subject to restrictions imposed by law enforcement or applicable law or regulations, Amwell will report any confirmed security breaches or compromises to impacted customers within one business day following the day on which Amwell qualifies the occurrence, not to exceed 5 business days following its knowledge of the event, or earlier if required by applicable law.

To the extent known, Amwell will present the impacted customer with documentation of the cause, remedial steps, and plans to prevent a recurrence within 5 business days following the day on which Amwell has knowledge of and qualifies the occurrence of the security breach or compromise.

Software Maintenance and Support

Definitions

Amwell System

An “Application” is a software environment that operates within the Converge hybrid care enablement platform ecosystem, delivering a differentiated set of unique capabilities via Amwell technology.
The “Amwell System” includes all hosted application(s) which are developed by and/or directly provided by Amwell to deliver the licensed services. For clarity, the Amwell System consists of all Amwell-developed microservices, SDKs, widgets and related services which are directly provided by and hosted by Amwell.

Documentation

Unless otherwise defined in Amwell’s agreement with a customer, “Documentation” is the published material authorized and distributed by Amwell that describes the Applications, and the installation and use of the Applications.

Enhancement

An “Enhancement” is a change or addition other than an Error Correction that improves the function, adds new function, or substantially enhances the performance of the Applications.

Error

An “Error” is a reproducible defect in the Amwell System that results in the Applications not functioning in material conformity with the Documentation.

Error Correction

An “Error Correction” is a change to the Applications or the Documentation, or a workaround, that is in a form that allows Amwell’s Applications to re-establish material conformity with the Documentation.

Level 1 Support

Amwell Level 1 Support includes:

- Available 24/7/365 to collect initial information about the reported issue

- Assessing the Severity of the reported issue for the purposes of determining the appropriate SLA response
- Assisting end users with the normal use of the system as described in the Amwell Documentation
- Troubleshooting and resolving basic issues
- Creating Salesforce tickets describing the issue, including the reproducible steps and additional information required to escalate to Level 2 Support when issues cannot be resolved by Level 1.

Client Assisted L1 Support includes:

- For Amwell products embedded in a Customer's electronic health record (EHR) system or other external system, "Level 1 Support" includes the Client's analysis required to rule out the Customer system as the source of the Error before reporting it to Amwell L2 Support for investigation. For all workflows involving the Amwell SDK, "Level 1 Support" includes the Client's analysis required to rule out the Customer system leveraging the SDK as the source of the Error before reporting it to Amwell L2 Support for investigation
- If Customer uses a third party's embedded workflow, unless otherwise agreed by the parties, "Level 1 Support" is the Third Party's analysis required by the third party to ensure such third party is not the source of the Error before reporting it to Amwell L2 Support for investigation. Once external systems have been ruled out as potential sources of an Error, Customer may escalate the suspected Error to Amwell Level 2 Support (defined below) for further investigation.

Level 2 Support

Level 2 Support includes:

- Attempting to reproduce and resolve the suspected Error on the Application leveraging administrative tools and functionality as described in the Amwell Documentation.
- Gathering additional information as required to reproduce the issue
- Assessing the Severity of the reported issue for the purposes of determining the appropriate SLA response

Escalating the issue to other functions within Amwell with the subject matter expertise to resolve the issue if it cannot be resolved by Level 2 Support.

Level 3 Support

"Level 3 Support" is the service provided to resolve reproducible Errors that are determined to be, or are highly probable to be, the result of a defect in the Applications, and which requires design engineering knowledge or technical expertise to isolate and resolve.

For Amwell products that are embedded in a Customer's electronic health record (EHR) system or other external system, that leverage a third party embedded workflow, or that leverage the Amwell SDK,

"Level 3 Service" is the service provided to resolve reproducible Errors that are determined to be, or are highly probable to be, the result of a defect in the Applications, and which requires design engineering knowledge or technical expertise to isolate and resolve. Once submitted by the Customer with all necessary information, these types of issues will be routed directly to Level 3 Support. After a Salesforce ticket is logged, the Amwell Support team will follow up directly with the Customer in the Salesforce ticket until resolution.

Maintenance Responsibility

Amwell will provide customers who subscribe to, and are current with respect to paying for, Maintenance and Support with updates to the Applications containing Error Corrections and/or minor or major Enhancements. Amwell will make these Error Corrections and Enhancements generally available to all Amwell hosted customers at or around the same time. Amwell will, at no additional cost to its hosting services customers, install Error Corrections and Enhancements on behalf of those customers. Amwell will perform any additional implementation and configuration in accordance with a Statement of Work at Amwell's then current rates. All Error Corrections and Enhancements are owned by Amwell, deemed part of the Applications, and licensed to customers in accordance with the terms and conditions of the applicable license agreement.

Support Responsibility

Product	Level 1	Level 2	Level 3
Amwell Applications (except products listed below)	Amwell	Amwell	Amwell
Cerner embedded	Cerner*	Amwell*	Amwell*
Customer EHR embedded and/or Single Sign On Integration	Customer	Amwell	Amwell

*Unless otherwise agreed by the parties

Third Party Content and Services

Amwell maintains support and maintenance arrangements with third parties that provide content or software for the Applications. When there is a problem with a third-party component which affects its Customers, Amwell works with the applicable third party in accordance with Amwell's arrangement for maintenance and support with that third party and provides support and maintenance for such component pursuant to such terms. Notwithstanding anything else set forth herein, Customer understands that the terms and conditions of the applicable third-party agreement accompanying such component control in the event of a conflict between the terms of such agreement and those contained herein.

Error Classification, Reporting and Response

Error Classification

Amwell shall respond to reported Errors according to their severity, as classified in accordance with Table 1.

Table 1 – Error Classification

Severity	Criteria
1	An Error that results in catastrophic failure of the Application or poses a significant, imminent risk to protecting the privacy of Protected Health Information.
2	An Error that results in the Application being usable, subject to major restrictions on its essential workflows, for which there are no workarounds.
3	An Error that results in the Application being usable, subject to major restrictions on its essential workflows, for which there are available workarounds, or an Error that disables non-essential workflows, regardless of whether a workaround exists.
4	An Error that results in inconveniences of the Application, which are not critical to its operation and for which there are workarounds.

Error Reporting and Response

Customers should report Errors in accordance with the standard reporting procedures described in Table 2 below. Errors that are properly reported to Amwell will be acknowledged by Amwell's Support team, who shall assess the Error and initiate appropriate corrective action by Amwell if needed.

Table 2 – Error Response

Severity	Error Response
1	Error reports will be acknowledged by Amwell within one hour. The issue will be worked on consistently until an official fix or adequate workaround is available. An action plan will be provided within 2 hours of notification if requested.
2	Error reports will be acknowledged by Amwell within 4 hours. The issue will be worked on consistently during office hours until an official fix or adequate workaround is available. An action plan will be provided within one (1) business day, if requested.
3	Error reports will be acknowledged by Amwell within one business day. Commercially reasonable efforts will be made to address prior to the next major release, or as otherwise communicated. An action plan will be provided within 10 business days if requested.
4	Error reports will be acknowledged by Amwell within one business day. Commercially reasonable efforts will be made to address by the next official release or as otherwise communicated.

Escalation Procedures

Amwell will staff a 24/7 support hotline for customers to report any Sev 1 or Sev 2 Errors. This Critical Issue Hotline can be reached at 833-315-0355 (press 1 for system outages (all Applications); or press 2 for 24/7 Critical Care Device and Telestroke provider support). When Amwell confirms a Sev 1 or Sev 2 Error has occurred, the Amwell incident response team will create an incident ticket and provide hourly updates to Amwell and Customer stakeholders. Updates will be provided via the Status Hub (https://status.amwell.com). Incident updates for the Home Application will be provided via the Status Page assigned to the customer (East - https://amwell-east.statuspage.io/access/login; or West - https://amwell-west.statuspage.io/access/login).

All support efforts will be performed on Amwell's premises. Should any on-site effort be required, customers agree to pay Amwell all travel expenses at Amwell's then per-diem rate unless such on-site support is the result of an Error. All expenditures will be approved by the customer in advance.

Documentation

Following an Error Correction or Enhancement, Amwell shall supply customers with a copy of any applicable modifications, supplements, or new documentation versions as soon as available.

Customer Error Reporting Guidelines

Amwell's obligations in the event of an Error are subject to its customers' adherence to the following guidelines:

- Customers must provide Amwell all information necessary for diagnosis of Errors within the response times set forth above.
- Customers, where appropriate, must provide experienced IT professionals and/or technical service representatives to collaborate with Amwell on troubleshooting and reporting Errors.
- Amwell may not be able to fix all Errors and may instead provide a workaround to an Error in-lieu of a fix.