



## HEALTHCARE SOLUTIONS, LLC.

### **Data Management Policy**

**Policy Owner:** Janna Friday

**Effective Date:** Feb 26, 2026

#### **Purpose**

To ensure that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization.

#### **Scope**

All Apricity Healthcare Solutions, LLC data, information and information systems.

#### **General requirements**

Apricity Healthcare Solutions, LLC classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

## **Data classification**

To help Apricity Healthcare Solutions, LLC and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data.

### **Confidential**

Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Examples include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation data

### **Restricted**

Apricity Healthcare Solutions, LLC proprietary information requiring thorough protection; access is restricted to personnel with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.

Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Slack messages
- Email

### **Public**

Documents intended for public consumption which can be freely distributed outside Apricity Healthcare Solutions, LLC. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

## **Labeling**

Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.

## **Data handling**

### **Confidential Data Handling**

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential data shall be encrypted at rest and in transit over public networks in accordance with the Cryptography Policy
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password (or equivalent, such as biometric) or passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures
- Hardcopy paper records shall only be created based on a business need and shall be avoided whenever possible
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

### **Restricted Data Handling**

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

### **Public Data Handling**

No special protection or handling controls are required for public data. Public data may be freely distributed.

## **Data retention**

Apricity Healthcare Solutions, LLC shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data.

Personally identifiable information (PII) shall be deleted or de-identified as soon as it no longer has a business use.

Retention periods shall be documented in the Data Retention Matrix in Appendix B to this policy.

## Data & device disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. Apricity Healthcare Solutions, LLC shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Apricity Healthcare Solutions, LLC requirements for secure data disposal shall be used for storage and processing of restricted or confidential data.

Apricity Healthcare Solutions, LLC shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of, disposal. Confidential and Restricted hardcopy materials shall be shredded or otherwise disposed of using a secure method.

Personally identifiable information (PII) shall be collected, used and retained only for as long as the company has a legitimate business purpose. PII shall be securely deleted and disposed of following contract termination in accordance with company policy, contractual commitments and all relevant laws and regulations. PII shall also be deleted in response to a verified request from a consumer or data subject, where the company does not have a legitimate business interest or other legal obligation to retain the data.

## Annual data review

Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy.

## Legal requirements

Under certain circumstances, Apricity Healthcare Solutions, LLC may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Apricity Healthcare Solutions, LLC legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with Apricity Healthcare Solutions, LLC's legal counsel to evaluate continuing requirements and scope.

## Policy compliance

Apricity Healthcare Solutions, LLC will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

## Exceptions

Requests for an exception to this Policy must be submitted to the Security Manager for approval.

## Violations & enforcement

Any known violations of this policy should be reported to the Security Manager. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

## Version history

Version	Date	Description	Author	Approver
3.0	Feb 26, 2026	Version 3.0	Janna Friday	Janna Friday
2.0	Aug 29, 2025	Version 2.0	Janna Friday	Janna Friday
1.0	Jul 28, 2025	Version 1.0	Kristy Elder	Kristy Elder

## **APPENDIX A - Internal retention and disposal procedure**

Apricity Healthcare Solutions, LLC's Executive Leadership Team is responsible for setting and enforcing the data retention and disposal procedures for Apricity Healthcare Solutions, LLC managed accounts and devices.

### **Customer Accounts:**

1. Customer accounts and data shall be deleted within sixty (60) days of contract termination through manual data deletion processes only when requested by the customer.
2. Patient account data will be deleted within three years of the date that the case or appeal is closed. Data will be retained for this three year time period for reporting/billing purposes and to provide clients with further information concerning appeals/billing questions as they arise.

### **Devices:**

Employee devices will be collected promptly upon an employee's termination. Remote employees will be sent a shipping label and the return of their device shall be monitored.

1. Collected devices will be cleared to be re-provisioned - or removed from inventory, Apricity Healthcare Solutions, LLC will work with IT providers to securely erase the device when reprovisioning.
2. Device images may be retained at the discretion of management for business purposes.

### **Destroying devices or electronic media**

In cases where a device is damaged in a way that Apricity Healthcare Solutions, LLC cannot access the Recovery Partition to erase the drive, Apricity Healthcare Solutions, LLC may optionally decide to use an E-Waste service that includes data destruction with a certificate. Apricity Healthcare Solutions, LLC will keep certificates of destruction on record for one year. Physical destruction can be optional if it is verified that the device is encrypted with Full Disk Encryption, which would negate the risk of data recovery.

Management will review this procedure at least annually.

## APPENDIX B - Data retention matrix

System or Application	Data Description	Retention Period
Apricity Healthcare Solutions, LLC SaaS Products (AWS)	Customer Data	Up to 60 days after contract termination when requested by client
Apricity Healthcare Solutions, LLC AutoSupport	Customer instance and metadata, debugging data	Indefinite
Apricity Healthcare Solutions, LLC Customer Support Tickets (Salesforce)	Support Tickets and Cases	Indefinite
Apricity Healthcare Solutions, LLC Customer Support Phone Conversations (TalkDesk)	Support Phone Conversations	Indefinite
Apricity Healthcare Solutions, LLC Security Event Data (Splunk)	Security and system event and log data, network data flow logs	On-Premise - Indefinite AWS Instance - 1 year
Apricity Healthcare Solutions, LLC Vulnerability Scan Data (Qualys)	Vulnerability scan results and detection data	6 months host (asset) data is retained until removed and purged from Qualys
Apricity Healthcare Solutions, LLC Customer Sales (Salesforce)	Opportunity and Sales Data	Indefinite
Apricity Healthcare Solutions, LLC QA and Testing Data (TestRail)	QA, testing scenarios and results data	Indefinite
Security Policies	Security Policies	1 year after archive
Temporary Files	AWS /tmp ephemeral storage	automatically when process finishes