

Security Overview

[Guardify](#), a division of VidaNyx Inc., is a cloud-based evidence management software solution created to securely manage and store sensitive video, audio and other digital files for Social Services, Health Care, Law Enforcement and Justice agencies and their multi-disciplinary team members. Originally designed to secure highly sensitive and legally protected child forensic interviews, Guardify's security architecture is based on the highest standards associated with HIPAA, CJIS, and other data security frameworks.

Guardify is an easy-to-use application that includes all the features, technical support, maintenance and training to empower interviewers, health care and social service providers, and law enforcement and legal professionals to do their work safely, simply, and securely.

Safely view, share and store interview videos



Save time and eliminate busy work

No more hours wasted burning DVDs and loading jump drives. Spend more time accelerating justice and healing.



Protect the most vulnerable

Secure your interviews with the highest CJIS, HIPAA and other security framework standards.



Control distribution and delivery

Instantly share or revoke privileges, track access and give permissions at the user level.




HIPAA Compliant

- Guardify has, from its beginning, undergone HIPAA assessments and third party penetration testing to confirm top security and privacy measures are validated by independent sources.
- All employees receive HIPAA training within their first week of employment and are required to complete annual security awareness and HIPAA training..
- A Guardify HIPAA risk assessment is conducted annually and we can provide a letter of attestation from our auditor upon request.

CJIS Ready

- Guardify first earned the Criminal Justice Information Services (CJIS) Ready Seal from ACE Seal Diverse Computing, Inc. in 2023.
- The CJIS ACE Division of Diverse Computing offers the first and only industry-standard process for evaluating CJIS-related products and services to ensure they align with the FBI's CJIS Security Policy which governs the creation, viewing, modification, transmission, dissemination, and storage of sensitive Criminal Justice Information.
- Seals are only awarded to agencies and companies after completing a meticulous audit and evaluation process that reviews systems, policies, and procedures.



powered by 

Guardify is built on Amazon Web Services in AWS GovCloud (US), ensuring all servers are running at optimal capacity, under ideal environmental conditions, with redundant sources of power and with servers located in more than one location to minimize risks related to natural disasters.

Security Measures

Guardify is architected using 13 layers of security to offer prosecutors, law enforcement officers, social workers, and child advocacy centers peace of mind to manage evidence like never before.

- Special attention was taken in ensuring that all data is private. Only authorized, licensed users who have been verified through multi-factor authentication can access the content.
- Access can be granted or removed in real-time. Users with the right authority level can grant or remove access to audio files, video files and associated attachments and annotations.
- All the data is encrypted and access goes through multiple levels of authentication. Guardify team members and technology providers are unable to access any content without the explicit consent and proactive sharing of content from a Guardify user.
- Guardify has also undergone HIPAA assessments and third party penetration testing to confirm top security and privacy measures are validated by independent sources.
- There is complete Chain of Custody tracking. At any time, users with the right authority level can see the historic access to the evidence, who currently has access, and who has accessed and handled or viewed the evidence - depending on Defense Privacy protocols and settings for your account..



Active and Passive Security Measures

Isolated Virtual Network for all information, digital files, cases, and data

- It is an isolated section of the Cloud → unless we grant access, no one else can access it.

Multi-factor Authentication

- Users need two credentials to be able to log in, with controlled access, roles, and protections on who can access, upload, download, transfer, and delete secure data. Each session expires within minutes of inactivity.

Data Encryption

- All sensitive data is automatically encrypted in transit and at rest, with rotating keys in the database, file system or object storage.
- Guardify is CJIS compliant, which includes use of FIPS 140-2 certified endpoints

Certificate Authority

- Provide certificates to encrypt data transmission.

Internal Firewalls

- Each account can restrict access to Guardify based on selected IP addresses.

Web Application Firewall

- Protects web applications from common web exploits.

Digital Rights Management (DRM)

- This applies to online video viewing and for video saved on a DVD or USB device that can only be played on a computer with access to the internet.
- Purpose of DRM is to prevent unauthorized redistribution of digital media.
- Restrict the ways users can copy content and access can be terminated at any time, even if the file is saved in a DVD or USB device.

Watermarking

- Hidden watermarks to identify the source (user and session) are embedded in Guardify videos played back in the Guardify system in case of abuse. If, for example, someone uses a cell phone camera to capture a second-hand recording of a video played by a Guardify user our watermark technology can identify who was logged in at the time of the unauthorized recording and what date and time it occurred.

Operating System Protection (Polyverse)

- Polymorphic Operating System creates a resilient system.
- Stops zero-day attacks like Spectre and Meltdown.
- Solves patching panic.

Physical Protection

- Data is in Guardify's infrastructure ("AWS region") consists of multiple, isolated, and physically separate and secure data centers within a broader geographic area.



Active and Passive Security Measures (continued)

Disaster Recovery & Business Continuity

- Recovery and Continuity Plans are reviewed annually
- Data is stored in AWS GovCloud S3 with 99.999999999% (11 9s) of durability, strong resiliency, and high availability, with backup in different geographic locations to address risk associated with natural disasters.
- Other services throughout the infrastructure are deployed across multiple availability zones to geographically separate any one point of failure.

Audits by third parties

- Guardify hires on an annual basis reputable third parties to audit our AWS cloud architecture and look for performance and security improvements on a continuous basis.
- HIPAA risk assessments are completed annually.

Penetration Testing by third parties

- Vulnerability assessment and identifying cybersecurity risks to the organization.
- Perform in-depth, real-world attack scenarios and technical security testing.
- Uses a variety of commercial and open source security testing tools.

User Access Auditing and Accountability

- We have controls on access in our design, login credentials, user roles, and permissions, and a complete record of who accesses data available for audit, if needed.

Role-Based User Management

- All the data in the system is controlled by the type of user, enabling maximum flexibility and access control.

Personnel Security

- Everyone is screened with a background check and we will submit to national fingerprint-based record checks and ensure state-approved background checks, where needed.

Security awareness training

- Employees receive training within their first week of employment and receive annual training on security awareness and HIPAA.

Incident Response

- We have safeguards to identify data breaches, data recovery plans, and policies in place governing our reporting of any data breach to appropriate authorities.

