



Vidanyx Overview

Vidanyx is a cloud-based video management software solution created specifically for Child Advocacy Centers to securely manage and store child forensic interview videos, enabling a smooth operation and ensuring long-term archiving.

Vidanyx is an easy-to-use digital tool to support forensic interview program management and includes all technical support, maintenance and training to support Child Advocacy Center and Multi-Disciplinary Team users. Multi-Disciplinary Teams using Vidanyx benefit from improved efficiency, effectiveness, collaboration, time and cost savings. Thanks to Vidanyx, victims of abuse and neglect never have to worry about their most violating truths getting into the wrong hands.

Peace of mind in managing your computing equipment:

Using Vidanyx to store forensic interview videos replaces the need for hardware such as local servers, external hard drives, DVDs and USBs, and related costs of renting off-site storage units, occupying on-site storage space, spending time managing access logistics and manual chain of custody, and other costs involved in outdated, lower-security storage measures. Vidanyx is a cloud-based system built on Amazon Web Services, 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

Vidanyx is architected using 13 layers of security to offer child advocacy centers and multi-disciplinary users peace of mind to manage forensic interviews 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 video files and associated attachments and annotations.

- All the data is encrypted and access goes through multiple levels of authentication. VidaNyx team members and technology providers are unable to access any content without the explicit consent and proactive sharing of content from a VidaNyx user.
- VidaNyx has also undergone HIPAA Readiness Audit and 3rd parties conduct Annual 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 a video, who shared or viewed the video, and who was granted or removed access to the associated attachments.

Detailed list of active and passive security measures:

Isolated Virtual Network for all ePHI data

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

Multi-factor Authentication

- User needs two credentials to be able to log in and the session expires within minutes of inactivity

Data Encryption

- All sensitive data is automatically encrypted with rotating keys in the database, file system or object storage

Internal Firewalls

- Each Center can choose to restrict access to VidaNyx based on selected IP addresses

Certificate Authority

- Provide certificates to encrypt data transmission

Role-Based User Management

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

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 VidaNyx videos played back in the VidaNyx system in case of abuse if, for example, someone uses a video camera to capture a second-hand recording of a video played by a VidaNyx user

Operating System Protection (Polyverse)

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

Disaster Recovery

- The data is stored in AWS servers, with backup in different geographic locations to minimize any risk associated with natural disasters

Penetration Testing by third parties (annual basis)

- 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

Architecture Audit by third parties (annual basis)

- VidaNyx 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.



To learn more about the foundational security layers of VidaNyx, watch a 6-min video here: <https://vidanyx.com/security/>.