VALT SECURITY + COMPLIANCE

INTELLIGENT VIDEO SOLUTIONS

INTRODUCTION AND BACKGROUND

Most IVS customers must comply with information security requirements and regulations, such as HIPAA and/or FERPA.

The Health Information Portability and Accountability Act of 1996 (HIPAA) applies to healthcare providers collecting and storing patient information electronically or otherwise. The HIPAA Privacy Rule protects sensitive patient information by establishing a set of patient rights and standards.

The Family Educational Rights and Privacy Act of 1974 (FERPA) applies to educational institutions that receive federal funds. This legislation protects the privacy of students' personally identifiable information (PII).

Both FERPA and HIPPA are designed to protect information of covered individuals and create mandates to prevent unauthorized access to that information.

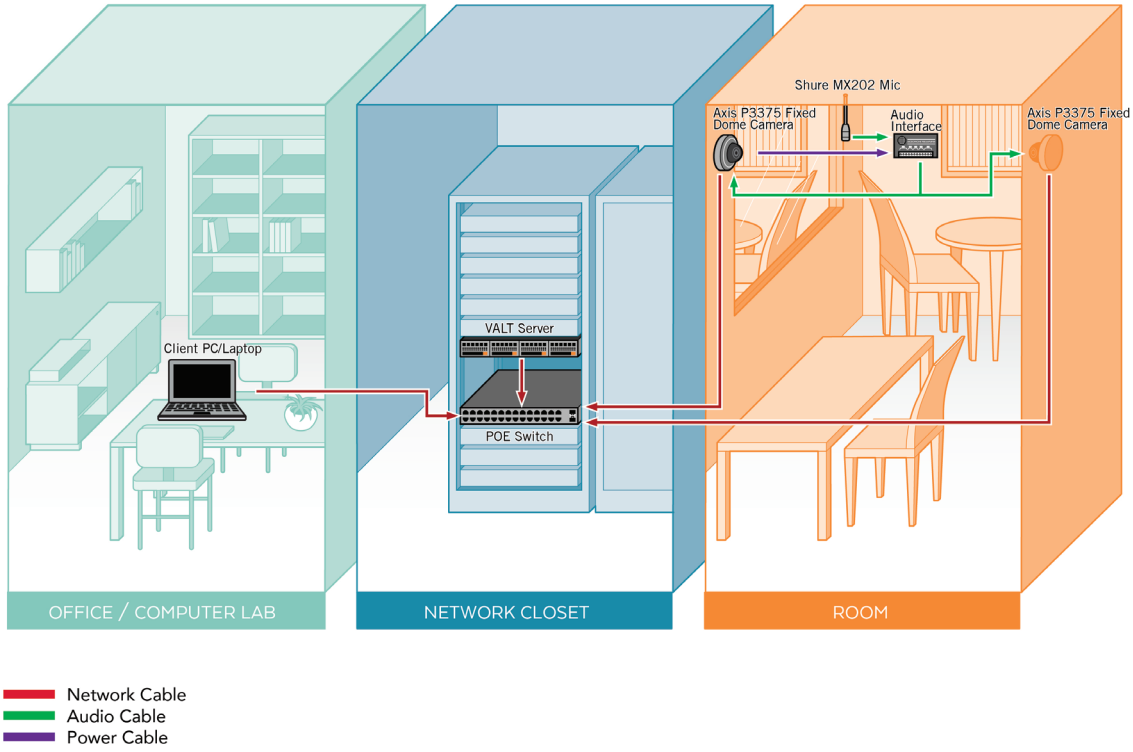
REGULATORY INTERPRETATION

HIPAA rules do "not assume the task of certifying software and off-the-shelf products" (p. 8352 of the Final Security Rule). Neither do they set criteria for, or accredit, independent agencies that do HIPAA certifications. This means no video software vendor can claim "full compliance or certification" to these acts.

It's also important to understand what IVS and VALT is and is not. VALT is an 'on premise' video solution, which means data lives in the customer's data center where security procedures are controlled and managed by the customer's network team.

IVS does not require access to video files, and thus does not require access to patient or student information, even when performing support or upgrade services. IVS does not maintain an active connection to any VALT server and such a connection can only be initiated, authorized and supervised by the customer.

With these important distinctions in mind, IVS would generally not be considered a 'Business Associate' but rather a 'software vendor'. That stated, IVS is willing to review any BAA, NDA or security audit documents.



REGULATORY COMPLIANCE

IVS developed specific features and system architecture to ensure no unauthorized person gains access to data protected under HIPAA and/or FERPA. The HIPPA Security Rule has three important types of safeguards detailed below:

TECHNICAL SAFEGUARDS

Implementation Specification	VALT Compliance
Implement a means of access control	Access to VALT is tightly controlled with granular permissions granted by a system administrator. VALT's login page is secured via TLS.
Implement Tools for Encryption and Decryption	VALT is compatible with the latest TLS encryption for all data in transit.
Introduce activity logs and audit controls:	VALT logs almost every activity performed in VALT.
Facilitate Automatic Log-off of PCs and Devices	A global automatic log-off variable can be configured within VALT.

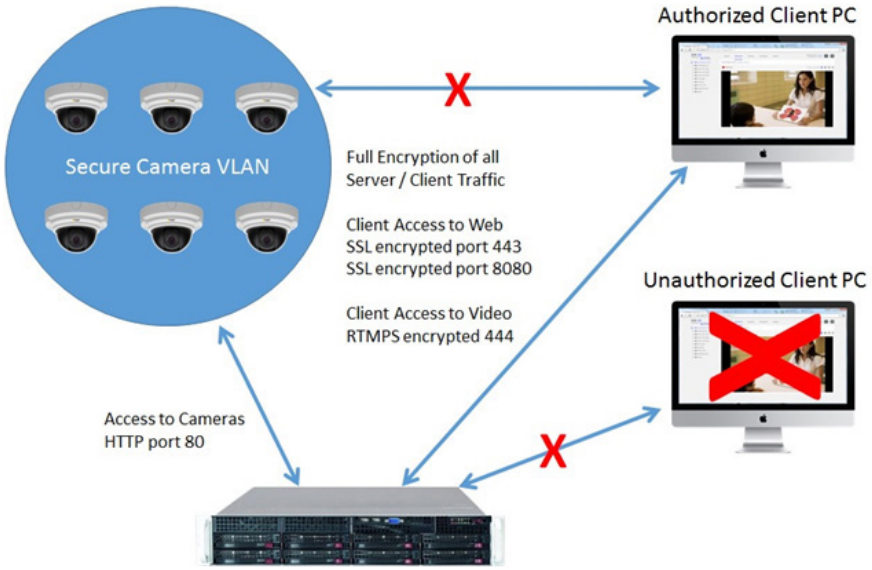
PHYSICAL SAFEGUARDS

Physical safeguards pertain to physical access to data. Since IVS never stores, processes or transmits data it is the responsibility of the customer to secure their facilities, workstations, and mobile devices.

ADMINISTRATIVE SAFEGUARDS

Administrative safeguards apply to the assessment, audit, reporting, and employee training procedures of the customer's organization. IVS employees are also trained to identify protected data and ensure it's never accessed without permission or removed from customer sites.

VALT SOLUTION: SECURITY & ENCRYPTION



VALT FEATURES

IVS implemented additional features to further secure data and help customers create operational procedures to maintain compliance.

Audit Trails: VALT logs all access to information and administrator actions. Each entry is date and time stamped. Examples include:

- **Login**: All successful and unsuccessful login attempts with user IP address
- **Camera/Room**: All access to live video streams by users
- **Recording**: Start/stop and scheduled recordings by user
- **Review**: Playback, clipping and downloading by user
- **Admin**: All admin changes

Password Encryption: VALT supports three authentication methods: Local, LDAP/LDAPS and SSO. Local passwords, if created, are encrypted in the VALT database. All VALT client traffic can be configured to use only HTTPS encryption.

Security and Permissions: Robust security and permission structure can be implemented to comply with any organization procedures. Access to each feature, video stream, recorded video asset and data is permission based.

Privacy Switches: VALT cameras and rooms can be paired with a physical privacy switch in or near the room, which places a black privacy mask over the video and mutes the audio so no observation or recording takes place. An optional light can indicate when a feed is 'live" and/or a recording is in progress.

LEARN MORE

tel. 262.746.9290 | email sales@ipivs.com | ipivs.com