VALT SECURITY + COMPLIANCE

HIPPA, FERPA AND DATA SECURITY REVIEW

ARCHITECTURE, FEATURES AND TOOLS TO MAINTAIN COMPLIANCE

December 2018

ipivs.com

INTELLIGENT
VIDEO SOLUTIONS

INTRODUCTION AND BACKGROUND

INTRODUCTION AND BACKGROUND

IVS serves many different markets with our VALT platform. While the use cases for video observation and recording may greatly differ one commonality between them all is the importance of data security and mandates to comply with specific regulations.

For our healthcare clients the Health Information Portability and Accountability Act of 1996 (HIPAA) is top of mind. The HIPAA Privacy Rule protects sensitive patient information by establishing a set of patient rights and standards that apply to healthcare providers collecting and storing patient information electronically or otherwise.

Those in education must be mindful of FERPA (Family Educational Rights and Privacy Act of 1974). This US federal legislation protects the privacy of students' personally identifiable information (PII). The act applies to all educational institutions that receive federal funds.

Both FERPA and HIPPA are designed to protect information of covered individuals and create mandates to prevent any unauthorized access to that information. Since many IVS customers are operating health clinics at postsecondary institutions open to the public with student practitioners they are required to comply with FERPA with respect to the education records of their students, and with the HIPAA Privacy Rule with respect to the health records of their nonstudent patients

REGULATORY INTERPRETATION

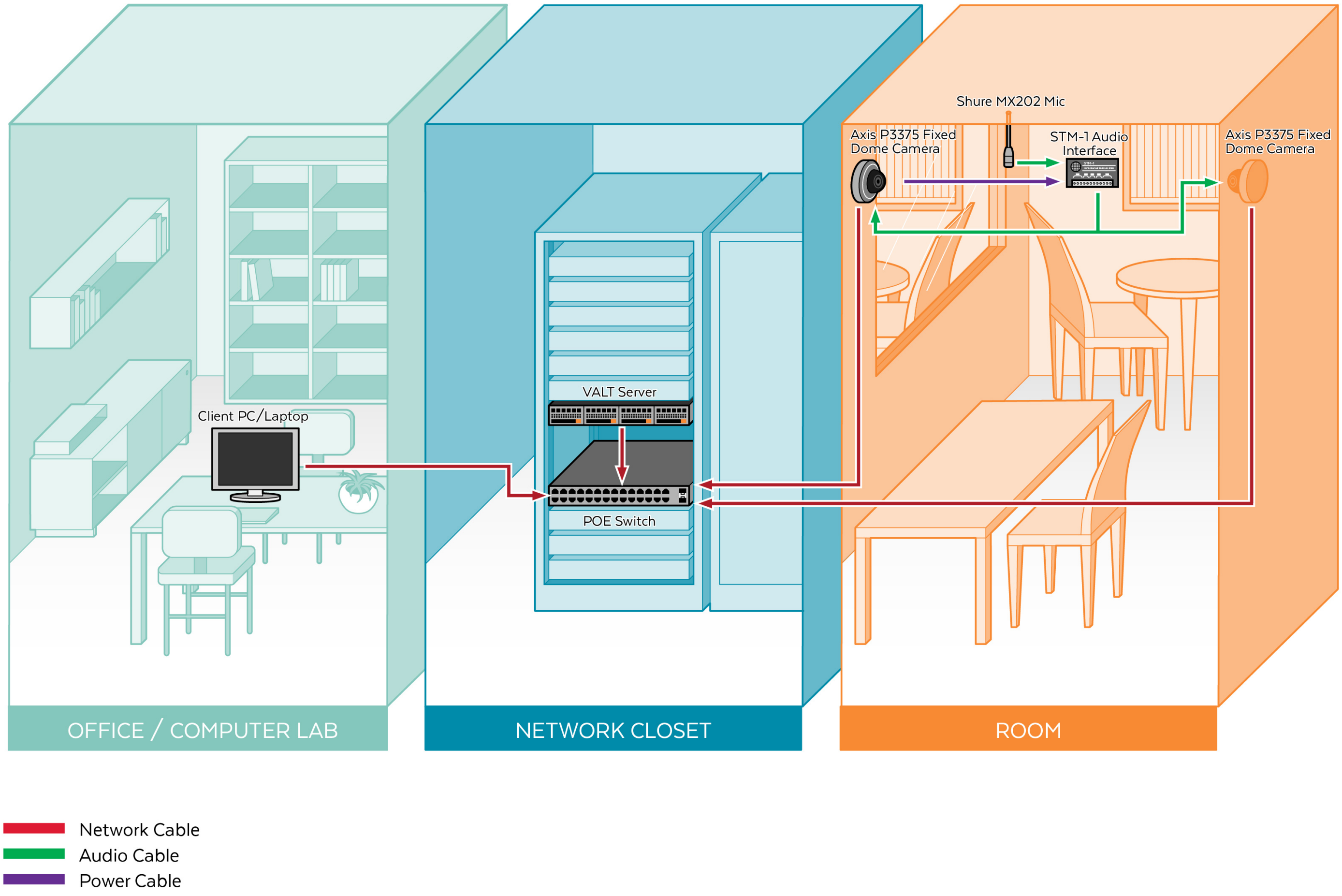
HIPAA rules do "not assume the task of certifying software and off-the-shelf products" (p. 8352 of the Final Security Rule) neither do they set criteria for or accredit independent agencies that do HIPAA certifications. This means no video software vendor can claim "full compliance or certification"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

It's also important to understand what IVS and VALT is and is **NOT**.

VALT is an 'on premise' video solution. This means that the data lives in the client data center where it can be under the control of the security procedures of the client's network term.

IVS does NOT require access to any video files and thus protected health or educational records. Even when performing support or upgrade services IVS does not require access to patient or student specific data. IVS does NOT maintain an active connection to any VALT server and such a connection can only be initiated, authorized and supervised by client personnel.

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

Since certain information about students and patients can be contained in video files maintained by VALT we take data security and compliance very seriously. IVS has developed specific features and system architecture to ensure no unauthorized person gains access to data protected under HIPPA and/or FERPA. The HIPPA Security Rule has 3 important types of safeguards detailed below.

TECHNICAL SAFEGUARDS

Implementation Specification	VALT Compliance
Implement a means of access control	All access to the VALT system must be granted by administrators via user groups. The login page is secured via TLS and access to any live video, recorded data or log is tightly controlled by granular permissions.
Implement tools for encryption and decryption	The security guidelines specifically state that NIST approved encryption standards must be applied to protected data if it travels beyond organization firewalled servers. To further ensure protection IVS encrypts data in transit using a sha-256 hash algorithm
Introduce activity logs and audit controls	Every user interaction and data activity is logged in VALT
Facilitate automatic log-off of PCs and devices	VALT administrators can set the auto log off the browser sessions per user group.

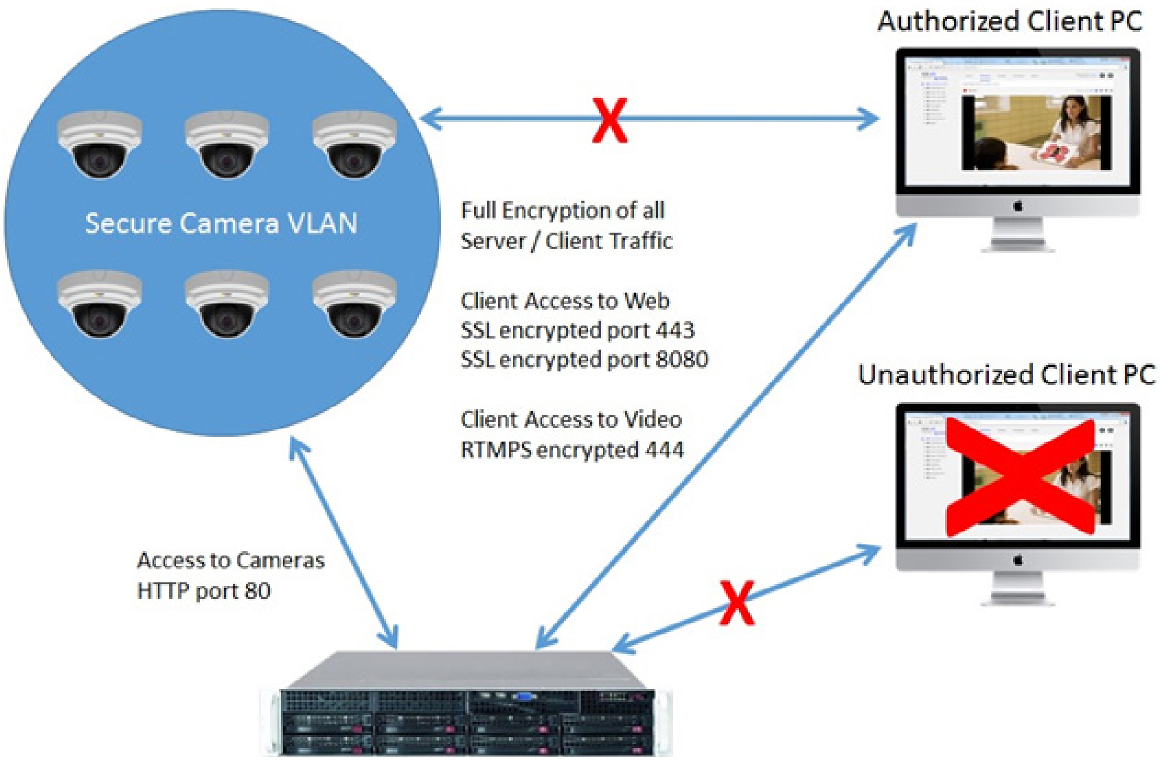
PHYSICAL SAFEGUARDS

These focus on physical access to the data. Since IVS never collects or transfers data it is the responsibility of the client to secure their facilities, workstations and mobile devices.

ADMINISTRATIVE SAFEGUARDS

These apply mainly to the assessment, audit, reporting and employee training procedures of the client organization. IVS also trains our employees on how to identify protected data and ensure its never accessed without permission or removed in any fashion from client sites.

VALT SOLUTION: SECURITY & ENCRYPTION



VALT FEATURES

IVS has implemented additional features and accessories to further secure data and help our clients create operational procedures to maintain compliance.

Password Encryption: The VALT solution can integrate with LDAP so no user passwords are stored on our system. IF passwords are created and stored on the VALT system they are encrypted in the VALT database. All client access to log into our browser based solution can be done over SSL encrypted ports.

Security and Permissions: VALT system administrators have granular access over every single feature, video stream, recorded video asset and data on our system. A robust security and permission structure can be implemented to comply with any organization procedures.

Audit Trails: VALT logs and makes available for search and sorting by system administrators the following information. Each entry is date and time stamped:

- Login: All successful and unsuccessful login attempts with user IP Address
- Camera/Room: All access to live video streams by user
- Recording: Start/Stop and Scheduled recordings by user
- Review: Playback, clipping and downloading by user
- Admin: Logs all admin changes

Privacy Switches: Any camera or room on the VALT system can be paired with a physical privacy switch in or near the room. This switch can place a black privacy mask over the video and mute the audio so that no observation or recording can take place. An optional light can indicate whether or not the feed is 'live" and/or a recording is in progress.