OpenEye®

A GUIDE TO OPENEYE WEB SERVICES

AND HIPAA COMPLIANCE

# OWS AND HIPAA COMPLIANCE

OpenEye Web Services (OWS) provides many benefits to IT administrators and users for managing and viewing video from recorders. If video or data containing information covered by HIPAA is transferred to or through OWS, it is important to understand how using OWS impacts your HIPAA compliance.

## WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA, is United States legislation that provides data privacy and security provisions for safeguarding medical information.

For the video security industry, HIPAA primarily applies to the collection, storage, and dissemination of Protected Health Information (PHI). PHI is anything that can identify a user such as the patient's name, address, video or pictures of the patient, medical records, etc.

## HOW IS OWS IMPACTED BY HIPAA?

HIPAA impacts OWS in many areas. These have been broken out into several key areas and discussed below.

### ENCRYPT ALL PHI DATA TRANSFERRED FROM THE RECORDER TO OWS

Any PHI or data that can compromise PHI must be encrypted when transferred from the recorder to OWS. This is achieved via HTTPS. Supported protocols and cipher suites are regularly evaluated and adjusted based on the latest industry best practices.

- OWS encrypts all non-video data transferred between OWS and the recorder
- OWS encrypts all streaming video transferred from the recorder to OWS
- OWS encrypts all video archive clips transferred to OWS from the recorder

### ENCRYPT ALL PHI DATA TRANSFERRED FROM OWS TO THE CLIENT

Any PHI or data that can compromise PHI must be encrypted when transferred from OWS to the client. This is achieved via HTTPS. Supported protocols and cipher suites are regularly evaluated and adjusted based on the latest industry best practices.

- OWS encrypts all non-video data transferred between OWS and the client
- OWS encrypts all streaming video transferred from OWS to the client
- OWS encrypts all video archive clips from OWS to the client

## ENCRYPT ALL PHI DATA STORED AT REST

Any PHI or data that can compromise PHI must be encrypted at rest. This requires data such as video archives to be encrypted when stored on OWS.

- All OWS video archive clips are encrypted at rest with a unique key employing strong multi-factor encryption. As an additional safeguard, the key itself is encrypted with a master key that is regularly rotated. The data itself is encrypted with 256-bit Advanced Encryption Standard (AES-256), one of the strongest block ciphers available.
- All images stored in OWS are encrypted at rest using the same approach and AES-256 cipher for video archive clips.

## COLLECT AND STORE LOGS OF ALL USERS WHO ACCESS PHI DATA

Anytime PHI is accessed by a user, logs must be created to allow auditors to trace who and when the information was accessed.

- OWS collects and stores logs of users and activity which touch PHI data

## ENSURE ALL PHI DATA IS SECURELY BACKED UP REGULARLY

All PHI data must be backed up regularly and transferred and stored in a secured environment.

- All OWS data is backed up daily and securely transferred to an offsite location
- Disaster recovery plans are in place to recover OWS data in the event of a catastrophic loss of data

## SERVERS AND DATA SHOULD BE SECURED

Servers and data should be secured accordingly using industry best practices. OpenEye Web Services utilizes a wide variety of industry best practices to ensure that the PHI data is protected. These include:

- Multi-factor authentication
- Servers are protected by 24/7 guards, access control and video surveillance
- Servers are protected by UPS systems, fire suppression and climate control systems
- Data is stored in multiple data centers across diverse geographic regions
- Data centers operate on the principle of high availability; that is, focus is placed on reducing single points of failure
- Data is stored on a private network that is not directly accessible to the internet
- Firewalls only allow access from specific servers to the data
- All customer data is logically compartmentalized through a tenant isolation layer

# MAINTAINING HIPAA COMPLIANCE WHEN USING OWS

Configured and used correctly, OWS can be deployed in environments covered by HIPAA. Review the following items and ensure each is properly configured.

## STREAMING VIDEO

There are several configurable options in OWS to determine how video will be streamed from the recorder to the client. Not all of the options available enforce the encryption of video. To ensure that all video is encrypted, OWS should be configured one of two ways:

1. Configure the recorder in OWS to steam video using the relay method for remote client connections. This is the easiest method to configure.
2. Configure the recorder in OWS to use Manual NAT for remote client connections. This option forces all clients to connect to the recorder using a static IP address. The IP address must be on a secured network shared with the recorder in order to connect.

## ALERT EMAILS / PUSH NOTIFICATIONS

Motion, Sensor, Analytic, Intrusion and other supported alerts may include a thumbnail image of each event to make it easier to identify if action is required. If the images contain patients in HIPAA protected areas (or other PHI data) the following should occur to ensure that HIPAA polices are not violated:

- Do not send alerts to users by email or by Push Notification. These methods are not encrypted and may violate HIPAA policies.
- If emails or Push Notifications are necessary, configure the recorder to not include alert images when events occur. The recorder can be configured to not send alert images to OWS thereby ensuring that PHI is not included in any emails that are sent out.

## USER MANAGEMENT

As with all applicable HIPAA computer systems at the install location, ensure that access to recorders, video clips, reports and other OWS functions is restricted to only those that require access. Be mindful that sharing data has the potential to violate HIPAA policies.

- Create unique user accounts for all OWS users
- Restrict OWS access to only those users who need access
- Ensure that the user granted access to OWS does not violate HIPAA polices
- Further restrict access to Video Archive and Alerts sections if they contain PHI

## Disclaimer

THE CONTENT PROVIDED IN THIS DOCUMENT IS OPENEYE'S INTERPRETATION OF HIPAA COMPLIANCE. OPENEYE STRONGLY ENCOURAGES YOU TO CONTACT YOUR HIPAA COMPLIANCE OFFICER TO DISCUSS THE INFORMATION PROVIDED.