# Data Encryption

| | |
|---|---|
| **Policy Name: Data Encryption** | **Effective Date: 07/04/2016** |
| **Policy Number: 4000** | **Revision Date: 08/01/2019** |
| **Department: IT** | **Author: Daniel Mos** |

**POLICY:** UnifyHR will encrypt all sensitive client data (PII, PHI) while at rest and in transmission. Sensitive client data refers to any data received from a client that has not been specifically designated as public by the client. Minimum key size should be up to date with current industry standards.

**PURPOSE:** Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a set of privacy and security requirements were established to protect certain health information. The regulations define protected health information (PHI) and standards for protecting this information including how it is held or transferred in electronic form. Due to these regulations, this policy establishes protocols for how the IT organization handles sensitive data at rest, in transmission, and while working.

**PROCEDURES:**

## Data at Rest

Sensitive data at rest is encrypted always. File level data is encrypted using PGP. Data in the SQL Server database is encrypted using Microsoft Transparent Data Encryption. Sensitive elements in the database are also encrypted at the field level.

## Data in Transmission

**Inbound Data -** UnifyHR can accept inbound client data either using SFTP, or FTPS. Both mechanisms encrypt the data in transmission. We also request that the client use our public PGP key to encrypt the data at the file level. Data is temporarily decrypted to be imported into our database, then the file is automatically encrypted using PGP. The data never exists outside of our firewalled production environment.

**Outbound Data -** Outbound data can be sent to clients using FTPS, SFTP, and HTTPS. We will also encrypt data at a file level upon request when using FTPS or SFTP.

**Email -** UnifyHR utilizes opportunistic TLS email encryption as well as an industry standard secure email product.

### Working with Sensitive Data

It is understood that data must be decrypted to perform work with it. The data is stored on encrypted media on company computers that may not be accessed without a unique user name and password. That data must be deleted immediately after the work is completed. Decrypted data should not remain on storage media while the employee is not actively working on it. Violations of this policy will result in disciplinary action.

This policy shall be reviewed for language and application on an annual basis following its last revision and shall be reviewed every year thereafter.

## Revision History

| Version | Date | Author | Summary of Changes |
|---|---|---|---|
| 1.0 | 12/15/2015 | Daniel Mos | Original |
| 1.1 | 07/05/2017 | Daniel Mos | Updates for Improvements/Changes in Process |
| 1.2 | 10/25/2018 | Jennifer Shaub | Added purpose statement |
| 1.3 | 08/01/2019 | Daniel Mos | Modified outbound data section |

## Approvals

| Version | Date | Approver | Summary of Changes |
|---|---|---|---|
| 1.0 | 07/04/2016 | Chris Heinefield<br>Craig Firestone | Original |
| 1.1 | 07/05/2017 | Chris Heinefield<br>Allen Gehrki | Updates for Improvements/Changes in Process |
| 1.2 | 10/26/2018 | Daniel Mos | Added purpose statement |
| 1.3 | 08/01/2019 | Daniel Mos | Modified outbound data section |