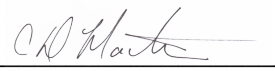
HARRIS COMPUTER SYSTEMS

CORPORATE TRANSMISSION SECURITY POLICY

Corporate Officer: Dwayne Martin, Vice President of CIT

Signature: 

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	08/18/16	Gina Martin/ Katie Rose	Major	Initial version of policy.	Todd Richardson
1.1	10/22/18	Katie Rose	Minor	Annual Review	Dwayne Martin
1.2	3/25/2020 *2019 review waived as approval for 2018 review cycle completed end of Q1 2019	Katie Rose	Minor	Annual Review, Added strong encryption standard, comment re: using customer email accounts	Dwayne Martin
1.3	3/24/2021	Katie Rose	Minor	Annual Review, Added reference to Communications, Data Sharing and Storage Policy and FIPS 140-2 Encryption standard; Inserted Definitions Document	Dwayne Martin

Harris Computer Systems
Corporate Transmission Security Policy

POLICY

To protect the confidentiality, integrity, and availability of Protected Health Information (PHI), Personally Identifiable Information (PII) or other Sensitive Information that Harris Computer Systems (Harris or "Company"), transmits over electronic communications networks.

PROCEDURE

1. When sending PHI, PII or other Sensitive Information over an electronic communications network, the PHI, PII or other Sensitive Information is sent in encrypted form and has controls to safeguard the integrity of the data. Sharing or storing PHI, PII or other Sensitive Information via Instant Messaging is strictly prohibited in accordance with the Corporate Communications, Data Sharing and Storage Policy. Email sent internally is encrypted, however email sent outside of the Company is not encrypted by default. T**herefore, it is vital that all email or email attachments containing PHI, PII or other Sensitive Information are sent using standard encryption features and processes.** If there is uncertainty that the communication is encrypted, the user must contact Corporate IT prior to corresponding using PHI, PII or other Sensitive Information. Further, at no time, should any Workforce Member utilize any email domains or instant messaging systems other than their work email or instant messaging systems (i.e., no public email domains such as gmail or yahoo accounts) to send PHI, PII or other Sensitive Information. For the purpose of best practice, Workforce Members should not use customer assigned email accounts for Company business without prior written manager approval.

Refer to this Knowledge Base Article (KBA45) for instructions on how to encrypt an email: https://harriscomputer.lightning.force.com/lightning/r/a3Q1500000017OaEAI/view

2. All transmissions including PHI, PII or other Sensitive Information should be sent via:

    a. Virtual private Network (VPN) connections that transmit PHI, PII or other Sensitive Information utilizing IPSec, SSL/TLS or SSH to establish temporary or permanent tunnels to the internal networks.) Ensuring proper authentication to access PHI, PII or other Sensitive Information will be accomplished through Mutual Authentication (in the case of SSL/TLS or SSH tunnels) or Authentication header (in the case of IPSec tunnels.)

    (ii) Ensuring proper integrity of PHI, PII or other Sensitive Information are accomplished by utilizing encryption with a

symmetric session key (in the case of SSL/TLS or SSH tunnels) or Encapsulating Security Payload (ESP) (in the case of IPSec tunnels).

b. Web applications will utilize Secure Hypertext Transfer Protocol (HTTPS) to ensure authentication and integrity of PHI, PII or other Sensitive Information.

(i) Web applications containing or transmitting PHI, PII or other Sensitive Information will utilize SSL over pre-defined ports. HTTP will be disabled at the server or blocked by local or network firewall access control configurations.

c. File Transfer Protocol (FTP) applications will use SFTP (enhanced with SSH), FTPS (utilizing SSL/TLS) or Secure FTP (SSH connection) to ensure authentication and integrity of PHI, PII or other Sensitive Information.

3. When accessing PHI, PII or other Sensitive Information through a remote connection, users are required to use a secure VPN connection. Under no circumstances may PHI, PII or other Sensitive Information be accessed through a public connection. If the ability to connect securely to VPN is not available or if there is uncertainty that a secure VPN connection is established, the user must contact Corporate IT prior to accessing PHI, PII or other Sensitive Information.

4. High encryption, at a minimum of Advanced Encryption Standard (AES) 256, and integrity controls are used when highly sensitive data such as PHI, PII or other Sensitive Information and passwords are transmitted over electronic communications networks. Companies that provide services to federal government agencies will utilize FIPS 140-2 compliant encryption.

Harris' integrity controls ensure that the value and state of all transmitted data is maintained, and the data is protected from unauthorized modification. Such controls include check sums, message authentication codes, and hash values(i) Ensuring proper authentication to access PHI, PII or other Sensitive Information will be accomplished through Mutual Authentication (in the case of SSL/TLS or SSH tunnels) or Authentication header (in the case of IPSec tunnels.)

(ii) Ensuring proper integrity of PHI, PII or other Sensitive Information are accomplished by utilizing encryption with a symmetric session key (in the case of SSL/TLS or SSH tunnels) or Encapsulating Security Payload (ESP) (in the case of IPSec tunnels).

b. Web applications will utilize Secure Hypertext Transfer Protocol (HTTPS) to ensure authentication and integrity of PHI, PII or other Sensitive Information.

Web applications containing or transmitting PHI, PII or other Sensitive Information will utilize SSL over pre-defined ports. HTTP will be disabled at the server or blocked by local or network firewall access control configurations.

c. File Transfer Protocol (FTP) applications will use SFTP (enhanced with SSH), FTPS (utilizing SSL/TLS) or Secure FTP (SSH connection) to ensure authentication and integrity of PHI, PII or other Sensitive Information.

1. When accessing PHI, PII or other Sensitive Information through a remote connection, users are required to use a secure VPN connection. Under no circumstances mayPHI, PII or other Sensitive Information be accessed through a public connection. If the ability to connect securely to VPN is not available or if there is uncertainty that a secure VPN connection is established, the user must contact Corporate IT prior to accessing PHI, PII or other Sensitive Information.
2. High encryption, at a minimum of Advanced Encryption Standard (AES) 256, and integrity controls are used when highly sensitive data such as PHI, PII or other Sensitive Information and passwords are transmitted over electronic communications networks. Companies that provide services to federal government agencies will utilize FIPS 140-2 compliant encryption.
3. Harris' integrity controls ensure that the value and state of all transmitted data is maintained, and the data is protected from unauthorized modification. Such controls include check sums, message authentication codes, and hash values.

DEFINITIONS

See attached policy definitions or click here.

REGULATORY REFERENCES

45 C.F.R. § 164.312(e)(1)