"Our Success is in Securing Yours"

Letter of Attestation for HIPAA Compliance

HIPAA Entity Type: Business Associate

Date: 12/09/2020

For Authorized Use Only

Company Sensitive and Proprietary

To Whom It May Concern:

In accordance with the Statement of Work, titled HIPAA Advisory, Assessment Services and Security Testing, and per the Letter of Agreement, dated June 26, 2020 ("LOA"), between RSI Systems, Inc. (dba RSI Security), its subsidiaries and affiliates (collectively, "RSI Security") and Neyenesch Printers ("Client"), RSI Security performed:

- Assessment of Neyenesch Printers' current security controls against 18 standards of the HIPAA Security Rule as applicable to a business associate;
- Review of Neyenesch Printers corporate and platform service networks; and
- Review of electronic protected health information (ePHI) data breach notification procedures.

The assessment and reviews were performed from July 2020 to December 2020. RSI Security:

- Received and reviewed documentation that described Neyenesch Printers' information security policies and procedures;
- Received and reviewed the security measures that are deployed as per the policies and procedures, in order to protect ePHI from unauthorized access or disclosures, as well as complying with the HIPAA Security Rule;
- Received and reviewed ePHI risk assessment reports; and
- Interviewed the personnel responsible for the information security and information technology management.

Based upon the representation from management as to the accuracy and completeness of information provided, the assessment procedures performed by RSI Security to validate such information, this letter provides reasonable assurance that Neyenesch Printers has designed and implemented administrative, physical, and technical safeguards in order to comply with the HIPAA Security Rule.

Sincerely,

Peter Phaneuf
Sr. Security Assessor
RSI Systems, Inc.

HIPAA Assessment Summary

About Neyenesch Printers

Neyenesch Printers was founded in 1899 and today provides a range of printing services to its customers using state-of-the-art equipment, including prepress, printing, finishing, binding and fulfillment. Because some of Neyenesch Printers' clients are HIPAA covered entities and had a need for printing jobs that contained medical record numbers, it was determined that Neyenesch Printers needed to comply with the HIPAA requirements applicable to HIPAA business associates.

About the HIPAA Security Rule

The Security Rule applies to health plans, healthcare clearinghouses, and to any healthcare provider who transmits health information in electronic form in connection with a transaction for which the Secretary of Health and Human Services has adopted standards under the Health Insurance Portability and Accountability Act (HIPAA) (the "covered entities") and to their business associates. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expanded the responsibilities of business associates under the HIPAA Security Rule.

The Security Rule specifies a series of administrative, technical, and physical security procedures for the entities to use to ensure the confidentiality, integrity, and availability of ePHI. The Security Rule requires entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. The entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

HIPAA Assessment Scope

- Neyenesch Printers corporate and platform service networks

HIPAA Compliance Status

✔	**Compliant** RSI Security performed an ePHI security risk analysis and Neyenesch Printers has deployed administrative, technical and physical safeguards in order to significantly reduce the data security risks to the ePHI received from the customers or customer associates.

HIPAA Assessment Description

Standard	Assessment Description
164.308(a)(1) Security Management Process	Neyenesch Printers has implemented the following: 1. Security policies and security controls to prevent, detect, contain and correct security violations; 2. Risk assessment process and mitigation strategies including automated procedures to discover vulnerabilities; and 3. Senior management support for information security programs.
164.308(a)(2) Assigned Security Responsibility	Neyenesch Printers has identified the security official who is responsible for the development and implementation of the ePHI data security policies and procedures.
164.308(a)(3) Workforce Security	Neyenesch Printers has implemented the following: 1. Authorization process and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information; and 2. Processes and procedures for electronic protected health information access termination.
164.308(a)(4) Information Access Management	Neyenesch Printers has implemented the following: 1. Authorization processes and procedures to ensure role-based access to ePHI databases and systems based on the job function; and 2. Access granting and modification procedures that include creating a unique username and authentication process.
164.308(a)(5) Security Awareness Training	Neyenesch Printers has implemented the following: 1. Procedures to provide periodic security updates to the personnel; 2. Security awareness training to the personnel upon hire and at least annually; 3. Procedures for guarding against, detecting, and reporting malicious software; 4. Procedures for monitoring log-in attempts and reporting discrepancies; and 5. Procedures for creating, changing, and safeguarding passwords.
164.308(a)(6) Security Incident Procedures	Neyenesch Printers has implemented an incident response plan that includes the procedures to: 1. Identify and respond to suspected or known security incidents; 2. Mitigate, to the extent practicable, harmful effects of security incidents that are known; and

	3. Document security incidents and their outcomes.
164.308(a)(7) Contingency Plan	Neyenesch Printers has implemented data backup and restore procedures.
164.310(a)(1) Facility Access Controls	Neyenesch Printers utilizes a secure internal data center infrastructure to host the ePHI application services and systems.
164.310(b) Workstation Use	Neyenesch Printers has deployed policies and procedures for the acceptable use of portals, technologies and computers (desktop and laptops) that are used to access ePHI.
164.310(c) Workstation Security	Neyenesch Printers has deployed policies and procedures for the management and security of computers (desktop and laptops) that are used to access ePHI.
164.310(d)(1) Device and Media Controls	Neyenesch Printers has deployed policies and procedures for the use of any removable media and secure storage of any media containing ePHI.
164.312(a)(1) Access Control	Neyenesch Printers has implemented policies and security measures to allow access only to the personnel or software programs that have been granted access rights to electronic information systems that maintain electronic protected health information: 1. Unique user identification and authentication; 2. Role-based access; and 3. Access session management and automatic logoff.
164.312(b) Audit Controls	Neyenesch Printers has deployed audit controls for recording and examining ePHI information system activity, especially when determining if a security violation occurred. Neyenesch Printers IT and information security personnel receive unusual activity alerts and perform review of audit logs periodically.
164.312(c)(1) Integrity	Neyenesch Printers does not require or allow interactive access to ePHI data. All ePHI data collection, transmission, storage, retrieval are performed via a secure application programming interface. Neyenesch Printers has deployed data and system backup and restore controls. Neyenesch Printers has deployed application, database, and system monitoring controls.
164.312(d) Person or Entity	Neyenesch Printers has implemented the following procedures: 1. Unique credentials with strong username and password known only

Authentication	to the authorized user; and 2. Two-factor authentication for all administrative and remote access to ePHI systems.
164.312(e)(1) Transmission Security	Neyenesch Printers has implemented the following: 1. Secure APIs and data transmission over secure HTTPS/TLS 1.2 protocols; and 2. Secure certificate based authorizations for API communications.