

Exhibit BContinued - Security Exhibit

This Security Exhibit (“Security Exhibit”) will be governed by Provider’s standard DocLib Hosting Services Agreement, dated on or about September 8, 2022, by and between Nevro and PICS DocLib, LLC (“Provider”) (the “Agreement”). Provider’s performance of the Services must be in accordance with the Agreement and this Security Exhibit. Capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement.

Nevro reserves the right to periodically propose modifications to this Security Exhibit to reflect current security practices, and upon mutual written agreement of the Parties, such modification will become effective upon any renewal of the then-current Statement of Work.

Nevro represents and warrants that it shall not disclose or provide Provider with access to any data (1) subject to the (a) Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999; (b) Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act and its implementing regulations (“HITECH”); or (c) Payment Card Industry (PCI) Data Security Standards (DSS); and (2) that is not in full conformance with all applicable data privacy legislation and regulations.

Purpose:

Provider will make commercially reasonable efforts to prevent the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or any other compromise of Nevro Data (collectively, a “Security Incident”). This Security Exhibit establishes the requirements necessary to maintain a security program and to identify the appropriate physical, operational, organizational and technical security measures for the protection of Nevro Data.

1. Information Security Management

1.1 Information Security Management System. Provider will maintain and continually make improvements to a documented information security management system in accordance with standard practices and accepted frameworks in Provider’s industry for the delivery of Services which its personnel are to be made aware of and comply with (“Information Security Management System”).

1.2 Testing. Provider will conduct at least annual third-party security tests on applications and infrastructure used to support the provision of Services to identify security vulnerabilities. Provider will provide summary reports of security testing to Nevro upon request.

2. Organizational Security

2.1 Information Security Responsibilities. Provider must have roles with clearly defined responsibilities for the administration of the Information Security Management System.

2.2 Security Policies. As part of administration of the Information Security Management System, Provider will create information security policies that will define responsibility for the protection of Nevro Data (“Information Security Policies”). The Information Security Policies will include requirements designed to monitor for compliance with Provider’s privacy/information security policies and procedures.

4/7/2022

3. Asset Classification

3.1 Asset Management. Provider will maintain an inventory of assets (computers, firewalls, routers, security devices, filing cabinets, etc.) that collect, store, process, access or transmit Nevro Data.*3.2 Asset Controls.* Provider will establish physical, organizational, and technical security controls designed to protect Nevro Data from unauthorized access and disclosure.

4. People Security

4.1 Provider Employees. Provider will make its employees aware of their responsibilities for maintaining effective security controls, particularly regarding the use of passwords, disposal of information, social engineering attacks, incident reporting, and the physical and technical security of users and company equipment through security awareness trainings. Provider will issue documented security policies, update them as necessary, provide security training, and obtain acknowledgement of these policies by all employees at least annually.

4.2 Background Checks. Provider must ensure that its employees involved in providing the Services have passed basic background checks designed to validate the completeness and accuracy of resumes, confirmation of professional qualifications, and verification of identity; where permitted by law these checks should also include checks of criminal history.

5. Physical and Environmental Security

5.1 Physical Access. Where Provider maintains a physical office location, Provider will maintain physical security controls designed to ensure that only authorized users have physical access to the network, critical systems and applications, server rooms, communication rooms and work environments. Provider will further provide protection for its physical facilities (e.g., through card readers, key cards or a manned reception area) from which Provider provides the Services. Provider will maintain controls to monitor for attempts at unauthorized access. Additional controls will be maintained to prevent or detect the removal of any such equipment.

5.2 Data Transfer. Provider will not transfer Nevro Data to any external or removable storage media without the prior written permission of Nevro.

6. Communications and Operations Management

6.1 Vulnerability/Patch Management. Provider will establish a vulnerability/patch management process that requires all systems used to provide the Services, including network devices, servers, and desktop/laptop computers, are patched against known security vulnerabilities in a reasonable period of time based on the criticality of the patch .

6.2 Secure System Configuration. Provider will establish controls to require that all systems used to provide Services are securely configured in a repeatable manner. This involves changes to default settings to improve system security (e.g., system “hardening”), changes to default account passwords and removal of unnecessary software or services/daemons. Additionally, employee devices used to interact or manage systems that provide the Services are to also be configured in a repeatable manner. Specific additional requirements beyond this Security Exhibit include:

6.2.1 Full/whole disk encryption; and

6.2.2 Remote data wipe and lock capability in case of lost/stolen device

6.3 Malware Prevention. Provider will implement detection and prevention controls to protect against malicious software and appropriate user awareness procedures. Provider will keep and update technical controls and must regularly evaluate all systems for the existence of malware.

4/7/2022

Provider will run real-time or regular scans of Provider's owned devices to detect viruses, malware, and possible security incidents.

6.4 Logging and Auditing. Provider will have in place a comprehensive log management program defining the scope, generation, transmission, storage, analysis and disposal of logs based on then current industry practices. The systems and the services will provide logging capabilities in accordance with the following principles:

6.4.1 the scope of logging and the retention policy will be based on a risk-based approach, with Windows user access logs retained for six (6) months and firewall logs maintained for thirty (30) days;

6.4.2 logs will be collected to permit forensic analysis on information security incidents;

6.4.3 logs will record administrative changes to the Services;

6.4.4 log records will be kept physically and virtually secured to prevent tampering;

6.4.5 passwords and other sensitive data elements will not be logged under any circumstances;

6.4.6 Provider will perform regular log analysis to evaluate security;

6.4.7 configuring all affected systems to provide real-time logging of any event that may indicate a system compromise, denial-of-service event, or other security violation, including notifying an administrator when pre-determined event thresholds are exceeded; and

6.4.8 protect logs from unauthorized access or modification.

7. Disaster Recovery and Business Continuity Planning

7.1 Programs. Provider must establish disaster recovery and business continuity programs for the Services, and such plans are designed to protect the confidentiality and integrity of Nevro Data during recovery operations. Provider will design the programs to prevent any reduction of security. Provider will test its disaster recovery and business continuity plan at least once in the calendar year.

7.2 Backups. Provider shall back up Nevro Data stored locally or processed by Provider through the use of backups. All backups should be encrypted prior to being stored.

8. Security Incidents

8.1 Incident Detection. Provider must establish and maintain an operational incident detection capability for responding to suspected or known Security Incidents or system breaches, and will develop a clearly documented incident response program, within six (6) months of the date of last signature to this Exhibit B, into its security governance program, which will incorporate a Security Incident response plan including methods to protect evidence of activity from modification or tampering, and to properly allow for the establishment of a chain of custody for evidence.

8.2 Incident Response. In the event of a Security Incident, Provider will utilize industry standard efforts to respond to the incident and mitigate the risk to Nevro and Nevro Data.

8.3 Incident Notification. In the event of a Security Incident, Provider will provide notice of the security incident to Nevro, which may be via email, within forty-eight (48) hours of Provider's determination that Nevro Data has been compromised.

9. Access Control

9.1 Authentication. Provider must use SSO mechanisms to interact with Nevro instance or assets (e.g., SAML 2.0, OKTA).

9.2 Centralization. Provider must have centralized authentication management mechanisms.

4/7/2022

9.3 Administrative Access. Provider must use multiple factors of authentication for all administrative access.

9.4 Brute-force Protection. Provider must implement controls on its internal systems designed to limit the capability of attackers to brute-force authentication endpoints.

9.5 Support Access. If Nevro allows Provider employees to access through an application support interface, that interface, at a minimum must (a) uniquely identify the Provider employee who used it, (b) record all interactions in a log that is available to Provider upon request, and (c) have its access list audited each quarter

9.6 User Passwords. Provider will provide training to employees reasonably designed to ensure passwords have sufficient complexity and expiration requirements or require an additional layer of security with multi-factor authentication.

9.6.1 Authentication and Two-Factor Authentication. “Two-factor authentication” means the authentication through the combination of something a person knows, such as a username and password, in combination with something a person has, such as a disconnected authentication token, or a biometric factor, such as a fingerprint. Provider must use multiple authentication factors where available, and Provider will use at least two-factor authentication to access accounts used to provide data hosting services. All administrative access by Provider employees must require two-factor authentication. If Provider is using Google Apps to manage their accounts, two-factor verification must be enabled.

9.6.2 Inactivity. All Provider devices must be locked after a reasonable period of inactivity.

9.6.3 Employee or Consultant Termination. At the time of the termination of an employee, contractor, or any third-party consultant, the terminated person’s access to the networks, systems, and accounts used to provide the Services and Support, and access to any Nevro Data, must be terminated.

9.6.4 Authorization. Provider shall not issue account credentials permitting access to Nevro Data to any third parties without Nevro’s prior written consent.

9.6.5 Network Access Controls. All networks Provider uses to provide the Services must be protected through the use of controls capable of blocking unauthorized network traffic, both inbound (ingress) and outbound (egress). Provider will maintain capabilities to monitor network traffic.

10. Data Security

10.1 Data Segregation. Provider logically separates, secures, and monitors production environments.

10.2 Credential Hashing. Provider must have appropriate algorithms in place for hashing secrets, including passwords and API tokens, both for Nevro’s accounts and for Provider accounts to access Nevro’s system. No credentials are to be stored in plain text or in a format that can be reversed.

10.3 Encryption.

10.3.1 Data both at rest and in-transit must be encrypted at all times using industry accepted cryptography standards.

10.3.2 Data in Transit. Provider must ensure that HTTPS is enabled in any web interface related to the product or service. Provider must disable non-encrypted transmission services (e.g., Telnet, FTP). Provider must have commercial certificates to provide Provider the option to utilize TLS 1.2 or greater for web facing applications.

131333118

4/7/2022

10.3.3 Data at Rest. Provider must have key management in place for high sensitivity data (e.g., key rotation, key encryption, access control, etc.). At a minimum, this includes:

10.3.3.1 Use Advanced Encryption Standard (AES) defined in FIPS 197.

10.3.3.2 Where different algorithms are used, they are to have comparable strengths e.g., if an AES-128 key is to be encrypted, an AES-128 key or greater, or RSA-3072 or greater could be used to encrypt it.

11. Privacy.

11.1 Provider represents and warrants that:

11.1.1 as of the date of this Agreement, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a (“FISA Section 702”).

11.1.2 no court has found Provider to be the type of entity eligible to receive process issued under FISA Section 702: (i) an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

11.1.3 it is not the type of provider that is eligible to be subject to Upstream collection (“bulk” collection) pursuant to FISA Section 702, as described in paragraphs 62 & 179 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (“Schrems II”), and that therefore the only FISA Section 702 process it could be eligible to receive, if it is an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4), would be based on a specific “targeted selector” i.e., an identifier that is unique to the targeted endpoint of communications subject to the surveillance.

11.2 Where possible Provider will use reasonably available legal mechanisms to challenge any request under FISA Section 702 for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific “targeted selector” (an identifier that is unique to the targeted endpoint of communications subject to the surveillance). Provider will use reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

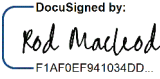

11.3 All employees are required to comply with Provider security and privacy policies and standards. Noncompliance is subject to disciplinary action, up to and including termination of employment.

11.4 Provider regularly reviews its collection, storage, and processing practices to prevent unauthorized access to Nevro’s system.

***** SIGNATURE PAGE FOLLOWS *****

4/7/2022

The parties here to have executed this Exhibit B (Security Exhibit) as of the date of last signature below by their duly authorized representatives.

Nevro Corp.	PICS DocLib
By: 	By: 
Name: Rod MacLeod	Name: Stephen Rosenthal
Title: CFO	Title: CEO
Date: 9/9/2022	Date: 9/9/2022

