Information Security Policy Exhibit

This Schedule Information Security Exhibit (this "Exhibit") sets forth information security requirements that ("Independent Physician") agrees to follow throughout the term of the Provider Agreement (the "Agreement") with Mitchell International, Inc. dba MCN ("Mitchell"). Independent Physician agrees that it is Independent Physician's sole obligation to (i) implement and maintain at least industry standard practices to secure its systems and data, including proprietary, confidential, personal, nonpublic, or other sensitive information that Vendor collects, receives, maintains or has access to under the Agreement (collectively, "NPI") against internal and external threats and risks; (ii) continuously review and revise those practices to address ongoing threats and risks; and (iii) comply with all applicable data privacy and protection laws, rules, and regulations ("Privacy/Security Laws").

1. Computer Systems Control.
    a. "Computer Systems" means any computer, network or system that is used by Independent Physician or its agents or employees to access, store or process any Proprietary Information.
    b. Independent Physician shall avoid visiting untrusted sites or foreign sites (statistical studies show many foreign sites are not secure) from its Computer Systems.
    c. Independent Physician shall not install illegal, malicious, or unlicensed software on its Computer Systems.
    d. Independent Physician must not test or attempt to compromise any information security mechanism put in place by Mitchell. Independent Physician must not utilize web-scraping, web-harvesting, or web-data extraction methods on any Mitchell software or systems, or otherwise alter any Mitchell software or systems.
    e. Restriction against Web Hosting – Independent Physician shall not host any web services from any computer that is used to access Mitchell's systems or store or process Proprietary Information.
    f. Email Use – if any Proprietary Information is ever sent over email, the email service used must have opportunistic TLS enabled over SMTP. Most major email providers (Gmail, Outlook.com, Hotmail, Live.com) provide these settings as default.
    g. Computer Systems must have antivirus software installed and enabled with auto-update enabled. Microsoft Windows and Apple MacOS provide a native solution to address this requirement if appropriately configured.
    h. Computer Systems must have auto-update enabled for security updates.
    i. Computer Systems must have firewall and hard-drive encryption enabled. Both Microsoft Windows and Apple MacOS provide native solutions to address these requirements, if appropriately configured.
    j. Web browsers utilized to access Proprietary Information must be kept current and Independent Physician will not lower the default security level settings.
    k. Passcode – A passcode of a minimum 4 characters must be enabled on all Computer Systems.
    l. Independent Physician will configure their computer systems to require usernames and passcodes, and require that such usernames and passcodes be used only by the person authorized, and not permit any sharing of passcodes or usernames.
    m. Wireless network access (e.g., IEEE 802.11x or similar technology) must be protected using an authentication and encryption method that follows standard IEEE 802.11i and is at minimum

AES-128 bit encrypted (WPA2).

2. Office Security and Travel Considerations.
    a. Printing. When printing Proprietary Information, only secure printer locations may be used. Any paper document containing Proprietary Information must be disposed of utilizing a shredding machine or service immediately after the case is closed.
    b. Be careful not to discuss Proprietary Information when in public places like hotel lobbies, public transportation, restaurants, and elevators. Viewing Proprietary Information on a computer screen or hardcopy report is prohibited when you are in a public place. You must be careful not to provide Proprietary Information in voice mail messages.
    c. When **working remotely**, Independent Physician must take due care not to leave any Computer Systems unattended. Do not leave computers visible in your car.
    d. Independent Physician shall avoid logging onto **public WiFi** using any Computer Systems. Public WiFi is considered unsafe and may be malicious.

3. Disposal
    a. Independent Physician agrees to **dispose** of all Proprietary Information at termination of contract or when retiring/disposing/handing-down any Computer System that stored Proprietary Information.
    b. **To dispose of data**, Independent Physician must permanently wipe Proprietary Information from the Computer Systems' hard drive utilizing a hard drive sanitization tool.
        i. Approved tools for Windows are: Active KillDisk Hard Drive Eraser, Eraser from Heidi Computers, Shredit for Windows, Disk Wipe, and Darik's Boot and Nuke.
        ii. Approved tools for Apple MacOS are: AweEraser for Mac, AweCleaner for Mac, DoYourData Super Eraser for Mac, and ShredIt X.

4. Reporting Incidents: All suspected disclosures or suspected compromise of Proprietary Information or any Computer Systems must be reported immediately to Mitchell's Information Security Department: Security@Enlyte.com.

5. Indemnity Clause. Independent Physician will hold Mitchell harmless from claims, damages, and expenses incurred by Mitchell resulting from a breach of the Independent Physician's security or any violation of the terms of this Schedule.

Information Security Standards for Customer Suppliers

Privacy

This Privacy Addendum, contains the terms and conditions relating to the processing of Personal Information under the Agreement.

I. Definitions

Capitalized terms used in this Exhibit that are not defined in this Section I shall have the meaning ascribed to them elsewhere in the Agreement, including this Privacy Addendum:

1. **"Customer"** means Customer of Mitchell International, Inc. dba MCN.
2. **"Data Protection Laws"** means all applicable laws and regulations regarding the Processing of Personal Information, including but not limited to the California Consumer Protection Act, the California Privacy Rights Act, Virginia Consumer Data Protection Act, and General Data Protection Regulations.

"Data Subject" means an identified or identifiable natural person.

"Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly with a particular individual, and includes any such information defined as Personal Information or Personal Data under any applicable Data Protection Laws. References to Personal Information or Customer Personal Information in this Privacy Addendum means Personal Information received from or collected on behalf of Customer.

"Process" or "Processing" means any operation or set of operations which is performed upon Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Services" shall have the same meaning ascribed to it in the Agreement, provided that if "Services" is not defined in the Agreement, "Services" means the products, services, or access and use of Supplier's software and/or hosted services provided by Supplier to Customer under the Agreement or any applicable schedule or statement of work thereto, and as described in Subsection V herein.

"Subcontractor" means any legal person or entity engaged in the Processing of Personal Information by Supplier.

"Supplier" Supplier shall be considered a Service Provider or a Processor, as those terms are defined under applicable Data Protection Laws.

II. Interpretation

This Privacy Addendum shall be incorporated into and form part of the Agreement. To the extent that the Privacy Addendum terms conflict with those elsewhere in the Agreement, the terms in this Privacy Addendum shall control to the extent of such conflict. For the avoidance of doubt, to the extent the Agreement includes more specific and stringent data protection or privacy requirements, the more specific and stringent requirements shall apply.

III. Use, Sharing and Destruction of Personal Information

A. Supplier understands and agrees that Personal Information shared by Customer with Supplier or collected by Supplier on behalf of Customer is only for the limited purpose of performing the Services under the Agreement and such Personal Information may not be used, maintained, stored or otherwise Processed except as necessary to perform the Services as allowed under the Agreement, pursuant to such further instructions as Customer may provide, or as may be required by law. Supplier may not combine any Customer Personal Information with personal information (as defined by Data Privacy Laws) it receives from another source, unless permitted by Data Protection Laws. Supplier must notify Customer of any obligation to use, maintain or store Personal Information to comply with a legal requirement. Supplier may not sell any Customer Personal Information and may not share any Customer Personal Information for purposes of cross-context behavioral advertising, as defined by the California Privacy Rights Act.

B. Upon Customer's request at any time and upon termination of the Agreement, Supplier must promptly destroy or return any Customer Personal Information including deleting or rendering unusable all electronic files and data that contain Personal Information. Supplier will require that any Customer Personal Information disclosed by the Supplier to a Subcontractor or other additional parties is also deleted in accordance with this provision. Supplier will provide a confirmation/certificate of destruction upon request within 5 business days of Customer's request, or other timeframe mutually agreed to by both parties.

C. Supplier may only share Customer Personal Information with additional parties if it has provided notice to Customer of such sharing and only to additional parties with whom it has a written agreement containing the same restrictions on the use, sharing and other Processing of such Personal Information as set forth in this Privacy Addendum, including provisions requiring the additional parties to adhere to the same level of security and privacy standards as required by this Privacy Addendum and compliance with Data Protection Laws.

D. Notwithstanding anything to the contrary in the Agreement, Supplier may be permitted to use aggregated and fully anonymized Personal Information for internal business purposes unrelated to the Services with Customer's consent.

IV. Supplier's Compliance Obligations

A. Supplier agrees to comply with all applicable Data Protection Laws. Supplier agrees at a minimum it will provide the same level of privacy protection for Customer Personal Information as would apply to Customer under applicable Data Protection Laws. Supplier will notify Customer if it

determines it can no longer meet any of its compliance obligations. Supplier will ensure that any of its employees or other individuals Processing Personal Information under the Agreement is subject to a duty of confidentiality with respect to the Personal Information.

B. Supplier agrees to assist Customer with and cooperate with Customer with regard to any of Customer's compliance obligations as it relates to the Personal Information, including, but not limited to: i) providing information to Customer on request which may be necessary to enable Customer to conduct any privacy impact assessments or other risk assessments required by law or internal company policy; or ii) to provide to Customer any Personal Information needed by Customer to respond to a consumer privacy request. To the extent permitted by law, Supplier will notify Customer promptly and act only upon Customer's instruction concerning any consumer privacy request including a request for disclosure, deletion or correction of Personal Information received directly from an individual concerning his/her Personal Information.

C. Supplier agrees that Customer may take any reasonable and appropriate steps to ensure Supplier uses Personal Information consistent with Customer's legal obligations including remediating any unauthorized use of Personal Information. Additionally, upon Customer's request, Supplier will (or cause its Subcontractors to) certify its compliance with the requirements of the Agreement and/or provide written responses to any reasonable questions submitted to Supplier by Customer, or an independent auditor.

D. If Customer shares with Supplier any de-identified or anonymized data, as defined under applicable law, Supplier agrees to comply with all requirements in Data Protection Laws relating to the use, sharing and maintenance of such data including all measures needed to prevent or prohibit the re-identification of the data. Specifically, Supplier shall not disassemble, translate, reverse engineer, or other decompile any de-identified or anonymized data or otherwise made any attempt to re-identify the data in order to identify any individuals or obtain any personally identifiable information through the use or manipulation of the data.

E. If the Supplier is providing Services subject to any additional legal requirements or regulations Supplier must also adhere to those requirements including, without limitation, any legal requirements or regulations that were not contemplated or in effect at the time of contracting.

F. Supplier will maintain a privacy program and data management framework to appropriately control and manage Personal Information, which program is appropriate for the nature of Supplier's business, the sensitivity or amount of Personal Information collected or used, and Data Protection Laws, self-regulatory principles or guidelines or other legal or contractual restrictions that apply to Supplier.

V. Additional Instructions for Processing

A. Subject matter and duration of the Processing of the Personal Information: Customer Personal Information will be Processed by Supplier in order to provide Customer with the products and/or services for the time period set out in the Agreement and applicable Schedule(s) (collectively, the "**Service Offering**"), and thereafter deleted or returned to Customer in accordance with Article III this Privacy Addendum.

B. The nature and purpose of the Processing of the Customer Personal Information: Customer Personal Information will be subject to automated and manual Processing operations by the Supplier, including, but not limited to transferring, collecting, storing, erasing or processing, as applicable, to provide Customer with the Service Offering.

C. The type of Personal Information to be Processed: The Personal Information Processed under the Agreement may include, but is not limited to, data elements and/or categories as identified on an applicable Schedule or other ordering document subject to and governed by the Agreement.