Subscription Services Agreement
General Terms and Conditions for
SecurePCI®, SecureHIPAA® and Secure Cloud Gateway®

1. Services.

1.1 Services description.

1.1.1 McKesson shall provide on a subscription basis the Services ordered by Customer for its Sites, which:

1.1.1.1 include certain Portal Services;

1.1.1.2 include if ordered, ASV External Vulnerability Scanning;

1.1.1.3 include if ordered, certain Security Services;

1.1.1.4 include if ordered, certain Additional Services; and

1.1.1.5 include if ordered, Onsite SCG Professional Installation.

1.1.2 As the Services are managed services provided by McKesson to many customers McKesson, at its sole discretion will, from time to time, make changes to the Services.

1.1.3 McKesson may provision the Services through its affiliates, agents, suppliers or subcontractors.

1.1.4 If the Services bundle ordered include the Secure Remote Access Services, Customer shall either: (i) promptly provide McKesson with the information required for the provisioning of such Services at the Site; or (ii) if Customer does not desire such Services at the Site, sign a waiver form (the "Waiver") provided by McKesson confirming that such Services are not to be provisioned to the Site. If Customer does not sign and return the Waiver within ten (10) days after the Waiver has been emailed or otherwise provided to Customer, Customer shall be deemed to have agreed to the Waiver. Customer acknowledges that the applicable fees and charges shall not change as a result of such Waiver.

1.2 Data Breach Protection Services. "Data Breach Protection Services" collectively refers to the "HIPAA Data Breach Protection Services" and the "PCI Data Breach Protection Services". The Data Breach Protection Services shall only apply to Data Security Events which are reported in writing to McKesson by a Merchant: (i) during the policy period of the insurance policy which backs McKesson's provision of the Data Breach Protection Services; and (ii) no more than sixty (60) days after discovery of the Data Security Event by the Merchant.

1.2.1 HIPAA Data Breach Protection Services (SecureHIPAA®).

1.2.1.1 The HIPAA Data Breach Protection Services (the "HIPAA-DBP-Services") include reimbursement of the following HIPAA Expenses subject to the maximum reimbursement amounts set forth in Section 1.2.1.4 below, in connection with a HIPAA Security Event:

1.2.1.1.1 HIPAA Civil Penalties;

1.2.1.1.2 HIPAA Legal Expenses; and

1.2.1.1.3 HIPAA Notification Expenses.

1.2.1.2 The HIPAA-DBP-Services shall: (i) be in effect from and after the Portal Start Date; (ii) apply to claims for breaches of which Customer receives written notice after the Portal Start Date; and (iii) not apply to claims for breaches which (a) Customer knew, or should have known, had occurred prior to the Portal Start Date, or (b) are not reported per Section 1.2 above; provided, however, in the event that Customer does not pay the applicable fees and charges when due, the HIPAA-DBP-Services shall be void as of the Portal Start Date, and shall not apply to any claims for breaches. Upon such failure to pay being remedied by Customer (the "Pay Remedy Date"), the HIPAA-DBP-Services shall: (i) be in effect from and after the Pay Remedy Date; (ii) apply to claims for breaches of which a Customer receives written notice after the Pay Remedy Date; and (iii) not apply to claims for breaches which (a) Customer knew, or should have known, had occurred prior to the Pay Remedy Date, and (b) are not reported per Section 1.2 above.

1.2.1.3 In order to file a HIPAA-DBP-Services claim, Customer shall follow McKesson' then current claim filing procedures by calling the McKesson support number listed in the Agreement or customer support guide, as applicable.

1.2.1.4 The maximum reimbursement of HIPAA Expenses is limited to $100,000 per HIPAA Security Event, regardless of the number of Covered Entities affected, and is further limited to:

1.2.1.4.1 $25,000 of HIPAA Legal Expenses per HIPAA Security Event, which limit is included within and not in addition to the limit set forth in Section 1.2.1.4 above; and

1.2.1.4.2 $25,000 of HIPAA Notification Expenses per HIPAA Security Event, which limit is included within and not in addition to the limit set forth in Section 1.2.1.4 above.

1.2.1.5 The Customer shall cooperate with McKesson and McKesson' contractors in: (i) enforcing any legal right to contest any HIPAA Civil Penalty and/or HIPAA Notification Expense; and (ii) enforcing any right of contribution or indemnity against any party other than the Covered Entity who may be liable for the HIPAA Security Event.

1.2.1.6 The HIPAA-DPB-Services shall not apply to:

1.2.1.6.1 any HIPAA Security Event known prior to or discovered outside the coverage period of the HIPAA-DBP-Services;

1.2.1.6.2 a Business Associate, unless the Covered Entity has been made legally liable for such HIPAA Civil Penalty, HIPAA Legal Expense, or HIPAA Notification Expense; or

1.2.1.6.3 any fraudulent, illegal, dishonest or criminal act committed by, at the direction of, or with the knowledge of any director, officer or owner of the Covered Entity.

1.2.2 PCI Data Breach Protection Services.

1.2.2.1 The PCI Data Breach Protection Services (the "PCI-DBP-Services") include reimbursement of the following PCI Expenses subject to the maximum reimbursement amounts set forth in Section 1.2.2.6 below:

1.2.2.1.1 Forensic Audit Expenses;

1.2.2.1.2 Card Replacement Expenses;

1.2.2.1.3 Card Association Assessments; and

1.2.2.1.4 Post PCI Security Event Expenses.

1.2.2.2 The PCI-DBP-Services shall: (i) be in effect from and after the Portal Start Date; (ii) apply to claims for breaches of which Customer receives written notice after the Portal Start Date; and (iii) not apply to claims for breaches which (a) Customer knew, or should have known, had occurred prior to the Portal Start Date, or (b) are not reported per Section 1.2 above; provided, however, in the event that Customer does not pay the applicable fees and charges when due, the PCI-DBP-Services shall be void as of the Portal Start Date, and shall not apply to any claims for breaches. Upon such failure to pay being remedied by Customer (the "Pay Remedy Date"), the PCI-DBP-Services shall: (i) be in effect from and after the Pay Remedy Date; (ii) apply to claims for breaches of which a Customer receives written notice after the Pay Remedy Date; and (iii) not apply to claims for breaches which (a) Customer knew, or should have known, had occurred prior to the Pay Remedy Date, and (b) are not reported per Section 1.2 above.

1.2.2.3 Customer does not have to be PCI DSS compliant to be eligible for the PCI-DBP-Services; provided, however, if Customer (or any Customer Affiliate) has had a previous breach at any time, or incurs a breach while eligible, Customer shall not be eligible (or re-eligible) for the PCI-DBP-Services until Customer's then current PCI DSS compliance is verified or re-verified, as applicable.

1.2.2.4 Only Level 2, 3, and 4 merchants (as such levels are defined by the PCI DSS) are eligible for the PCI-DBP-Services.

1.2.2.5 In order to file a PCI-DBP-Services claim, Customer shall follow McKesson' then current claim filing procedures by calling the McKesson support number given in the Agreement or customer support guide, as applicable.

1.2.2.6 Maximum reimbursement of PCI Expenses.

1.2.2.6.1 Per Merchant PCI-DBP-Services. For a Customer with only one (1) MID, the maximum reimbursement of PCI Expenses is limited to: (i) $100,000 per Merchant annually; (ii) a per occurrence maximum of $100,000; and (iii) an annual aggregate maximum of $100,000.

1.2.2.6.2 Per MID PCI-DBP-Services. For a Customer with multiple MIDs, the maximum reimbursement of PCI Expenses is limited to: (i) $100,000 per MID per year; and (ii) a per occurrence maximum reimbursement of $500,000, and an aggregate annual maximum reimbursement of $500,000.

1.2.2.7 Account Manager. Customer's receiving the Per MID PCI-DBP-Services as referenced in Section 1.2.2.6.2 above, shall also be assigned a named Account Manager to assist with Customer's PCI Compliance activities.

1.2.2.8 The PCI DPB-Services shall not apply to:

1.2.2.8.1 a Level 1 merchant as defined under the PCI DSS; or

1.2.2.8.2 any PCI Security Event that arises out of a Merchant allowing any party other than its employees to hold or access cardholder information.

1.2.3 Mitigation. Customer agrees to take reasonable steps to prevent Data Security Events and to mitigate losses arising out of such events, including, without limitation, following the procedures required by Card Associations and the Regulator, as applicable, in the event of a Data Security Event. In the event of a Data Security Event, Customer agrees not to take any action, or fail to take any action, assume any financial obligation, pay any money or incur any expense in connection with the Data Security Event that prejudices the rights of McKesson under this Agreement without first obtaining McKesson' prior written consent, or some, or all, of the Customer's claim may not be covered by the Data Breach Protection Services.

1.3 Continuous Compliance Management. "Continuous Compliance Management" ("CCM") For use only with a Level 3 or Level 4 Merchant Site, and includes the following:

1.3.1 Managed PCI eLearning. Bulk upload of Users and assignment of training and policy on a monthly basis. A McKesson account manager will work with Customer on User changes and assignment of training courses and policies.

1.3.2 Managed Security Policy. Provides templates for PCI Security Policy by SAQ type. Policy will be adjusted to the Customer's environment and published on the applicable learning management system. A McKesson account manager will work with Customer to update the policy on a quarterly basis to incorporate changes to the Customer's environment.

1.3.3 Managed ASV External Vulnerability Scanning. A McKesson account manager will work with Customer to: (i) determine IP type (i.e. Static or Dynamic); and (ii) review ASV scans and provide remediation guidance based on scanning results on a quarterly basis.

1.3.4 Managed PCI Self-Assessment Questionnaire. A McKesson account manager will work with Customer to: (i) determine the SAQ which is applicable to Customer's Bank Card processing; and (ii) provide annual guided SAQ completion assistance.

1.3.5 Managed Penetration Testing Guidance. Annual penetration testing guidance for Customers that have multiple corporate owned Sites. A McKesson account manager will work with Customer and McKesson's Consulting Services Division to schedule this activity.

1.4 Onsite SCG Professional Installation.

1.4.1 Summary. If Customer has ordered Onsite SCG Professional Installation, then at Customer's request McKesson will provide technicians in the United States *(subject to availability and geographic restrictions)* for onsite installation of the applicable Services.

1.4.2 Installation procedures.

1.4.2.1 The firewall will be configured and shipped direct to the Site from McKesson.

1.4.2.2 The McKesson technician will be scheduled to visit the Site to complete the installation.

1.4.2.3 The fee includes a single dispatch of the McKesson technician. Each additional dispatch will include a minimum of one (1) additional hour of working time per each additional dispatch at McKesson' the then current rate per hour.

1.4.2.4 The McKesson technician will perform Secure Remote Access Services software installation.

1.4.2.5 The McKesson technician will not perform any facility modifications or other construction activities (e.g. no drilling into, or mounting of equipment on, wall, etc.).

1.4.2.6 Upon completion, the McKesson technician will have a Customer or Customer Affiliate representative sign an acceptance document confirming the successful installation.

1.4.3 Installation requirements and conditions.

1.4.3.1 Customer is responsible for providing the McKesson Technician will all licenses related to, and all passwords for, Customer's computers, routers, networks, etc. needed to perform the installation.

1.4.3.2 McKesson is not providing any software or software licenses for Customer's computers, routers, networks, etc. McKesson will not install any unlicensed software whether provided by Customer or any other party.

1.4.3.3 Customer, Customer Affiliate or User delays will be a billable event, including delays due to: (i) any outage of Customer's network; (ii) any power outage at the Site; (iii) any outage due to an improper operating environment at the Site, i.e. temperature, moisture, dust or dirt; etc.

1.4.3.4 The requirement for ladders over eight (8) feet will need to be noted in the service request prior to dispatch.

1.4.3.5 The building and work area is to be free of hazardous materials

1.4.3.6 Regular business hours are 7:00 am to 6:00 pm Monday through Friday in the time zone local to the installation Site.

1.4.3.7 There is a 1.5x charge for any work completed outside of regular business hours.

1.4.3.8 Holidays include New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day and Christmas Day. Service requests on these days are billed at 2x the regular rate.

2. McKesson Equipment. Some of the Services will involve Customer's use of McKesson Equipment. All McKesson Equipment provided by McKesson to Customer in connection with certain of the Services, shall at all times be and remain the sole property of McKesson, and when provided to Customer is provided solely on a leased basis. Customer shall bear all risk of loss of or damage to all McKesson Equipment provided to Customer, from the time of delivery to Customer until return delivery to McKesson or McKesson's designee, ordinary wear and tear excepted.

3. Restrictions. McKesson. Customer may not copy the Services, in whole or in part. Use is limited to Customer's internal use of the Services. The Services shall not be re-sold, rented, distributed or transferred by Customer to any third party. Customer will not use the Services for the benefit of third parties. Customer shall not itself, nor permit any other party to: (a) reverse engineer, reconstruct or discover any source code or underlying ideas or

algorithms or file formats or programming or interoperability interfaces of the Services by any means whatsoever; (b) remove, alter, cover or obfuscate any end-user agreement, copyright notices or proprietary legends; (c) develop methods to enable any third party to use the Services, in whole or in part; (d) incorporate all or any portion of the Services into any other service or product or create any derivative work; (e) use the Services for timesharing, service bureau, subscription service, or rental use; or (f) publish or otherwise disseminate any results of any tests or operating results of the Services.

4. Customer responsibilities. (a) Customer shall: (i) provide McKesson with documentation and information, including the MID for each Site, as may be required by McKesson to perform the Services; (ii) provide trained staff to assist as necessary and to answer questions that may arise in connection with the installation, provisioning, and ongoing performance of the Services; and (iii) be responsible for use of the Services by its Users. (b) Customer shall obtain, install and maintain any equipment, software and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, server, software, operating systems, networking, web servers, Internet access, long distance and local telephone service. Customer shall maintain the compatibility of such equipment, software and ancillary services with the Services. (c) Customer shall not tamper with, alter, modify or otherwise rearrange the Services nor shall it permit or assist others to abuse or fraudulently use the Services including but not limited to using the Services: (i) in any manner which interferes unreasonably with the Services or McKesson' provision of similar services to other parties; (ii) for any purpose or in any manner directly or indirectly in violation of applicable laws; or (iii) in violation of any third party rights. (d) Customer shall use the Services only in compliance with McKesson' then current standard use policies, then current end user agreement(s) of McKesson and certain McKesson suppliers, and all applicable laws and regulations, and third party rights.

5. Support.

5.1 Initial login. For each User that will receive the Services, McKesson shall guide Customer and its Customer Affiliates' Users through the initial login. After the completion of the initial login, McKesson support will apply, as needed.

5.2 McKesson support. McKesson support includes:

5.2.1 Guiding Users through the Portal's base functionality.

5.2.2 Guiding Users through routine issues concerning the Services.

5.3 Changes.

5.3.1 McKesson may change the fees and charges at the start of the next Renewal Term by providing Customer at least ninety (90) days prior written notice. Customer may, if such changes are not acceptable, terminate this Agreement at the end of the applicable Initial Term or Renewal Term upon at least sixty (60) days' prior written notice to McKesson.

5.3.2 The fees and charges are based on the Services facilitating the management of compliance with the Payment Card Industry Data Security Standard (the "PCI DSS"), Version 3.0 November 2013. In the event of changes to the PCI DSS, McKesson may change the fees and charges upon at least ninety (90) days prior written notice to Customer. Customer may, if such changes are not acceptable, terminate this Agreement by providing written notice of termination to xMcKesson not later than thirty (30) days after receiving such notice from McKesson, with the effective date of termination to be the ninetieth (90^{th}) day after Customer has received such notice from McKesson.

6. Moves, adds, changes. In the event Customer requests any moves, additions or other changes (collectively called "MAC(s)") to the Services *(examples: a change of the location(s) of the Site(s) where the Services are delivered; or adding new Site(s) to receive the Services)*, Customer shall provide McKesson at least thirty (30) days prior written notice of the requested MACs, and McKesson will provide Customer a quote of the applicable fees and charges per McKesson s Change Order process. No MACs will be implemented until a written Change Order is signed by the Parties.

7. Term and termination.

7.1 Term of Agreement. The term of this Agreement shall commence on the Effective Date and shall remain in effect for so long as any Site Term(s) remain in effect.

7.2 Site Term. The initial term for a Site (the "Site Initial Term") commences on the Billing Date for such Site and continues thereafter for the period of time set forth in the Agreement. After the Site Initial Term, the Site Term shall automatically renew for successive twelve (12) month renewal terms (the "Site Renewal Term(s)") on each anniversary of the applicable Billing Date. The Site Initial Term and Site Renewal Terms are collectively called the "Site Term".

7.3 Termination of a Site. Either Party may terminate the Site Term for a given Site effective at the end of the applicable Site Initial Term or Site Renewal Term, by providing the other Party at least one hundred twenty (120) days' prior written notice. After termination for a given Site, this Agreement shall remain in effect for the remaining Sites.

7.4 Termination of Agreement. This Agreement shall terminate upon the termination of all Site Terms pursuant to Section 7.3 above.

7.5 Effects of Termination.

7.5.1 Site. Upon termination of the Site Term for a Site: (i) McKesson shall cease to provide the Services to the Site; (ii) Customer shall immediately pay all fees and charges owed hereunder applicable to the Site; (iii) Customer shall immediately return to McKesson all McKesson Equipment (in good working order, ordinary wear and tear excepted) and all McKesson Software applicable to the Site; and (iv) each Party shall destroy or promptly return to the other Party the other Party's Confidential Information, except to the extent that such Confidential Information may be retained by a Party for purposes of performing its obligations under this Agreement with respect to other Sites that continue to receive Services.

7.5.2 Agreement. Upon termination of this Agreement: (i) McKesson shall cease to provide all Services; (ii) Customer shall immediately pay all fees and charges owed hereunder; (iii) Customer shall immediately return to McKesson all McKesson Equipment (in good working order, ordinary wear and tear excepted) and all McKesson Software; and (iv) each Party shall destroy or promptly return to the other Party the other Party's Confidential Information.

8. Franchisee Data. When a Customer's Site is operated as a franchisee location of a franchisor with which McKesson has a business relationship, McKesson may disclose to such franchisor data about such Customer Site related to compliance, network security, or WiFi connectivity and use.

9. Services Statistics. Customer agrees that McKesson may gather and utilize statistical information gathered in connection with the Services and the data processed by the Services (the "Services Statistics"), however, McKesson will only utilize the Services Statistics: (i) in a manner that will not identify Customer or any Merchant as the source thereof; (ii) in a form where the data is de-identified; and (iii) in compliance with all applicable laws and regulations.

10. Definitions. The following terms shall have the meanings set forth below, unless the context requires otherwise:

10.1 *"McKesson Equipment"* means any equipment deployed to Customer to enable McKesson to provide the Services which is either: (i) owned by McKesson; or (ii) is owned by McKesson' agents, suppliers or subcontractors, and as between McKesson and Customer shall be deemed owned by McKesson.

10.2 *"McKesson Software"* means the firmware, plug-ins and software provided by McKesson (which may include third party software) that is included in or associated with the Services, along

with all updates, upgrades, patches, and bug fixes thereto. The McKesson Software may include features that prevent use of the related Services after the expiration or termination of the applicable Site Term, and/or upon improper use of the McKesson Software.

10.3 *"Bank Card"* means a financial transaction card, including a debit card, credit card or prepaid card, issued by a Card Association or a financial institution as a member of a Card Association.

10.4 *"Business Associate"* means a contractor, subcontractor, and other contracted entity, not otherwise excluded, that are not an employee of a Covered Entity but that requires access to Protected Health Information as part of providing services to the Covered Entity. Business Associate does not include: life insurance companies; health insurance companies; employers liability or workers compensation insurers; hospitals; health plans (including HMO, company health plan, and certain governmental programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs; schools or educational institutions; state agencies; law enforcement agencies; or municipalities and municipal offices.

10.5 *"Card Association"* means each of the following entities formed to administer and promote cards: MasterCard International, Inc.; VISA U.S.A., Inc.; VISA International, Inc.; Discover Financial Services; American Express; JCB International Credit Card Company, Ltd., and any similar credit or debit card association that is a participating organization of the PCI Security Standards Council.

10.6 *"Card Association Assessment"* means: (i) a monetary assessment, fee, fine or penalty levied against a Merchant by a Card Association as the result of a PCI Security Event, or a security assessment conducted as a result of a PCI Security Event; and (ii) shall not exceed the maximum monetary assessment, fee fine or penalty permitted upon the occurrence of a PCI Security Event by the applicable rules or agreement for such Card Association.

10.7 *"Card Replacement Expenses"* means the costs that the Merchant is required to pay by the Card Association to replace compromised Bank Cards as the result of a PCI Security Event, or a security assessment conducted as a result of a PCI Security Event.

10.8 *"Covered Entity"* means any of the following entities, not otherwise excluded, which is subject to the requirements of HIPAA and has ordered HIPAA DBP-Services under this Agreement: Host Health Care Providers meaning doctors, clinics, psychologists, chiropractors, allied health providers, nursing homes, pharmacies, and dentists. Covered Entity does not include: life insurance companies; health insurance companies; employers liability or workers compensation insurers; hospitals; health plans (including HMO, company health plan, and certain governmental programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs; schools or educational institutions; state agencies; law enforcement agencies; or municipalities and municipal offices.

10.9 *"Customer"* is the Party named on the first page of this Agreement which is a Covered Entity and/or a Merchant.

10.10 *"Customer Affiliate"* means any entity that is a Covered Entity and/or a Merchant, and which directly, or indirectly through one or more intermediaries, controls or is controlled by, or is under common control with Customer.

10.11 *"Data Security Event"* collectively means any HIPAA Security Event or PCI Security Event. Continuous or repeated actions or exposure to substantially the same general harmful condition, injury or damage shall be deemed a single Data Security Event. All HIPAA Expenses and PCI Expenses resulting from the same, continuous, related or repeated event or which arise from the same, related or common nexus of facts, will be deemed to arise out of the first such Data Security Event.

10.12 *"Forensic Audit Expenses"* means the costs of a security assessment conducted by a Qualified Security Assessor approved by a Card Association or the PCI Security Standards Council to determine the cause and extent of a PCI Security Event. For the Forensic Audit Expenses to be reimbursed, the Customer must be notified in writing by Customer's Card Association or Acquiring Bank, that the Forensic Audit is mandatory.

10.13 *"HIPAA"* means the Health Insurance Portability and Accountability Act of 1966, Public Law 103-191, as amended, and the rules and regulations promulgated thereunder.

10.14 *"HIPAA Civil Penalty"* means regulatory fines and penalties assessed by the Regulator against the Covered Entity as the result of HIPAA Security Event, and does not include: criminal penalties; economic damage to any party; legal and other expenses; punitive or exemplary damages; the cost to restore consumer identities or monitor or verify the creditworthiness, credit accuracy or damage to credit of any consumer; or the cost of hardware or software upgrades.

10.15 *"HIPAA Expenses"* means the sum of all HIPAA Civil Penalties, HIPAA Legal Expenses, and HIPAA Notification Expenses incurred as the direct result of a given HIPAA Security Event.

10.16 *"HIPAA Legal Expenses"* means attorney fees and all other reasonable fees, costs and expenses directly associated with the investigation, defense, appeal or settlement of a HIPAA Security Event with the Regulator. HIPAA Legal Expenses shall not include: expenses incurred in the defense, appeal or settlement of any civil or criminal action by or against an entity other than the Regulator; declaratory judgment expenses; and independent monitoring or Cumis counsel expenses.

10.17 *"HIPAA" Notification Expenses"* means all expenses associated with mandatory notification following a HIPAA Security Event as required under the HIPAA Breach Notification Rule.

10.18 *"HIPAA Security Event"* means the actual or suspected unauthorized access to or use of "Protected Health Information" (as defined under HIPAA), arising out of a Customer's possession of or access to such Protected Health Information.

10.19 *"Merchant"* means a party that accepts Bank Cards in the course of its business.

10.20 *"Merchant Identification Number"* or *"MID"* is a unique number assigned to a Merchant account to identify it throughout the course of processing activities.

10.21 *"PCI Expenses"* means the sum of all Forensic Audit Expenses, Card Replacement Expenses, Card Association Assessments, and Post PCI Security Event Expenses, incurred as the direct result of a given PCI Security Event.

10.22 *"PCI Security Event"* means the actual or suspected unauthorized access to or use of cardholder information, arising out of a Merchant's possession of or access to such cardholder information which has been reported: (i) to a Card Association by such Merchant; or (ii) to such Merchant by a Card Association.

10.23 *"Portal"* means the portal through which Customer accesses various features of the Services.

10.24 *"Portal Start Date"* means the date on which McKesson provides the credentials for the use of the Portal at the applicable Site.

10.25 *"Secure Remote Access Services"* means the McKesson services that enable Users to connect to their corporate Workstations from outside their office.

10.26 *"Post PCI Security Event Expenses"* means reasonable fees and expenses incurred by the Merchant with prior written consent for any service: (i) specifically approved in writing, including without limitation, identity theft education and assistance and credit file monitoring; and (ii) which approved service is provided (a) by or on behalf of the Merchant within one (1) year following the discovery of the PCI Security Event to a cardholder whose cardholder information is the subject of the PCI Security Event, and (b) for the primary purpose of mitigating the effect of the PCI Security Event.

10.27 *"Regulator"* means the Department of Health and Human Services, Office of Civil Rights or any governmental body or official authorized by them; responsible for regulating and enforcing HIPAA

and the rules and regulations promulgated thereunder against Covered Entities.

10.28 *"Remote Access Destination Site"* means a single Customer or Customer Affiliate Site which Remote Access Services to the Customer Workstations at that location.

10.29 *"Secure Cloud Gateway"* or *"SCG"* means the security device which is installed at each Site for which a Premium Services Bundle is ordered, and which includes both McKesson Equipment and McKesson Software.

10.30 *"Services"* means the services ordered by Customer and provided by McKesson on a subscription basis pursuant to this Agreement.

10.31 *"Services Statistics"* is defined above.

10.32 *"Site"* means a physical Customer or Customer Affiliate location that will receive the Services, with each Site identified by a unique MID.

10.33 *"Site-to-Site Services"* means the McKesson services that provide connectivity between distinct Merchant networks which may reside in offices that are in different physical locations.

10.34 *"User"* means each individual Customer or Customer Affiliate employee, contractor, agent or representative who is authorized by Customer and McKesson to receive and use Services under this Agreement.

10.35 *"Workstations" are computers located at Customer or Customer Affiliate Sites that are made accessible remotely using the Secure Remote Access Services.*