verizon

RISK ANALYTICS for PRIVACY MANAGEMENT +

Part I: Rates and Charges.
Part II: Service Description and Requirements.
Part III: Terms and Conditions.
Part IV: Definitions

Part I: Rates and Charges.

1. **Rates and Charges**.

   1.1 Customer will pay the annual recurring charges, one-time fees, monthly recurring charges ("MRC") and non-recurring charges ("NRC") for Verizon Risk Analytics for Privacy Management, as specified in the applicable Service Order or Online Terms, and at the following URL: http://www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.

Part II: Service Description and Requirements.

1. **Verizon Risk Analytics for Privacy Management Solution Components.** Verizon Risk Analytics for Privacy Management will provide a privacy management software platform (the "Software Platform") and certain services required to support the Software Platform (collectively, "Verizon Privacy Management Components").

   1.1 **Software Platform.** The Software Platform takes as input a feed of raw transactions (e.g. Electronic Medical Records access logs, and associated reference data) supplied by Customer systems; processes the transactions utilizing a variety of predictive modeling, risk scoring, data mining techniques, and identifies patterns that are readable by analysts.

      1.1.1 **Predictive Modeling and Risk Scoring Software and Processes.** Verizon Privacy Management predictive modeling system is a high-volume, streaming data reduction platform that supports the receipt of near real-time data. The predictive modeling software applies domain-specific, predictive models, configurable edit rules, artificial intelligence and risk scores to identify data patterns and outliers.

      1.1.2 **Case Management Module.** Verizon's case management module extracts potentially privacy violation cases for more detailed review. Analysts collect the data necessary to substantiate further disposition of an extracted case. Verizon will establish key performance indicators to measure performance metrics from the analyst level through the global enterprise level.

      1.1.3 **Reporting Tools.** Verizon Privacy Management includes standardized and ad-hoc reporting, data mining tools, and a large-volume data warehouse for trending and analytics. Warehoused suspect privacy violation alerts (based on the rules and algorithms implemented as per the Customer's requirements) and case management data will be available to investigators for post data analysis and additional case development. Examples of regular reports include: Trend Analytics, Key Performance Indicators/Performance Metrics, and Intervention Analysis/Effectiveness.

   1.2 **Verizon Privacy Management Installation Services.** In addition to Verizon Privacy Management Components, Verizon shall provide certain supplementary installation services (the "Installation Services") to assist in the implementation and utilization of Verizon Privacy Management. The following are the required:

      1.2.1 Interface Specification and Physical Development.

      1.2.2 Implementation.

2. **Technical Requirements.**

2.1 **Data Source Connectivity.** Verizon currently uses the Internet along with X.509 certificates across a Virtual Private Network (VPN) or TLS/SSL secured Web Service to establish and secure connectivity to Verizon Privacy Management Systems.

Part III: Terms and Conditions.

1. **Limitation of Liability.** Notwithstanding anything to the contrary in the Master Terms the total liability of Verizon to Customer in contract, warranty, tort or otherwise (including negligence, strict liability, misrepresentation, and breach of statutory duty) in connection with the provision of Risk Analytics for Privacy Management is limited to the lesser of (a) direct damages proven by Customer or (b) the aggregate amounts due from Customer to Verizon for the six months prior to accrual of the latest cause of action for which the limitation of liability under this clause is being calculated.

2. **Customer Liability.** Customer is solely liable for claims, actions, demands, losses, expenses, damages, liabilities, costs (including, without limitation, interest, penalties, reasonable attorneys fees and expenses) and judgments arising out of Customer's use, or failure to use, Verizon Privacy Management. Customer's liability obligations hereunder will survive termination of these terms and conditions. Nothing set forth under these terms and conditions shall be deemed to waive or limit rights or remedies of Verizon under common law or applicable laws, rules, orders or regulations, including without limitation common law indemnity, contribution or impleader.

3. **WARRANTY DISCLAIMER.** VERIZON PRIVACY MANAGEMENT IS PROVIDED "AS IS" AND "AS AVAILABLE", WITHOUT WARRANTY OR REPRESENTATION OF ANY KIND. VERIZON AND ITS SUPPLIERS AND LICENSORS MAKE NO REPRESENTATIONS, WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, WITH RESPECT TO VERIZON PRIVACY MANAGEMENT, ITS AVAILABILITY, QUALITY, PERFORMANCE OR THE RESULTS OF ITS USE. VERIZON SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OR FITNESS FOR A PARTICULAR PURPOSE. ANY INFORMATION OBTAINED VIA VERIZON PRIVACY MANAGEMENT IS AT CUSTOMER'S OWN RISK.

4. **Additional Representations and Warranties and Disclaimers.**

4.1 Customer acknowledges and agrees that Verizon is in no way responsible or liable for any loss or damage to Customer data. Customer is solely responsible for backing up data that is to be used with Verizon Privacy Management prior to sending any such data to Verizon. Customer is solely liable for claims, actions, demands, losses, expenses, damages, liabilities, costs (including, without limitation, interest, penalties, reasonable attorneys fees and expenses) and judgments arising out of Customer's failure to back up any such data.

4.2 Customer acknowledges and agrees, that Verizon Privacy Management Components, as defined in Exhibit A, are information management tools only and that they contemplate and require the involvement of Customer's learned intermediaries. Customer further acknowledges that Verizon Privacy Management is performed at the direction of the Customer, and that Customer is responsible for its actions or failures to act upon information provided by Verizon.

4.3 Customer is responsible for determining what constitutes a privacy violation. Verizon shall have no liability for Customer's interpretation of or compliance with any law and shall be entitled to rely on Customer's interpretation of or representation of compliance with any law.

4.4 Customer further acknowledges and agrees that Verizon has not represented that Verizon Privacy Management or Verizon Privacy Management Components have the ability to diagnose disease, prescribe treatment, or perform any other tasks that constitute the practice of medicine or of other professional or academic disciplines.

4.5 Customer warrants that it owns all right, title, and interest in and to, or has the license for and the right to grant Verizon access to, any programs, systems, data, materials or other information furnished by Customer to Verizon for the purpose of enabling Verizon to perform Verizon Privacy Management.

4.6 Use of Verizon Privacy Management, like other network-based services, carries certain security risks to the systems and networks of Customer, Verizon and third parties including, but not limited to: misuse, unauthorized access; alterations; theft; destruction; corruption; and attacks ("Occurrences"). Customer warrants that it will use S/MIME protocol with AES 128-bit encryption to transmit all data that it sends to Verizon in order to perform Verizon Privacy Management. Customer will use firewalls, passwords, access restrictions, patch installation and management and such additional security measures as Customer deems appropriate, based upon

reasonably anticipated risks, to protect from Occurrences all Verizon Privacy Management traffic, Customer facilities, equipment, software, data and systems located on Customer's premises or otherwise in Customer's control and used in connection with Verizon Privacy Management. Customer is responsible for all security measures and compliance with all state and federal data privacy and security laws and other laws and regulations, which pertain to the preparation, storage, transmission or analysis of the Customer's data even if Customer uses a third party to configure and implement them.

5. **Intellectual Property.**

5.1 All right, title and interest, including but not limited to copyrights, patents, pending patent applications, trade secrets, trademarks, trade names and all other intellectual property rights, in (i) Verizon Privacy Management ; (ii) any hardware or software provided; (iii) any modifications thereto or derivative works thereof; or (iv) any invention relating to or improvement in Verizon Privacy Management conceived in or made in the course of or as a result of Customer's performance under these terms and conditions; shall at all times remain the exclusive property of Verizon, its affiliates and/or its licensors or suppliers (as the case may be).

5.2 Verizon may modify, deconstruct, reassemble and/or process the data provided by Customer in order to provide Verizon Privacy Management.

5.3 Customer grants Verizon the right to use all data provided by Customer necessary to access, open, use, transmit, modify, store and process such data in order to provide Verizon Privacy Management and to transfer data to affiliates of Verizon and other entities necessary to provide or to facilitate the provision of Verizon Privacy Management in accordance with the terms and conditions of the Business Associate Agreement, Exhibit B, where applicable.

5.4 Verizon Privacy Management contemplates the processing and analysis of data that originates within the United States.

Part IV: Definitions. In addition to the definitions identified in the Master Terms, the following administrative charge definitions apply to Risk Analytics for Privacy Management: http://www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm

Exhibit A
Installation Services

1. **Objectives / Success Criteria.** The objectives of Verizon Privacy Management are as follows:
   - Proactively identify user activity that conflicts with the minimum necessary standard or established role / access policies, or constitutes inappropriate behavior
   - Design an operational workflow to accelerate remediation of identified privacy risks within the provided dataset
   - Define the value proposition and quantify the benefits of a privacy monitoring solution
   - Develop a plan to operationalize the solution across multiple applications and locations

2. **Approach and Timeline.** Verizon Privacy Management consists of four primary work efforts:
   - **Project Planning**
     - Review a proposed high-level project and resource plan
     - Define and assess source data content and format
     - Determine data handling details in a Technical Kick-off session
   - **Data Acquisition and Mapping**
     - Set up Verizon's privacy monitoring application platform and software
     - Acquire Customer source data (EMR, reference, etc.) as defined in the Technical Kick-off session
     - Map source data to the privacy monitoring application's run-time input formats
     - Analyze and validate the source data for completeness and consistency
     - Gather and analyze policy and role access information
   - **Configuration and Workflow Design**
     - Apply role and policy information to configure privacy monitoring algorithms
     - Test, tune, and refine algorithms to minimize false positives and generate actionable results
     - Train staff on Graphical User Interface (GUI)
     - Design an operational workflow to remediate privacy risks using the privacy monitoring application
   - **Results and Workflow Assessment**
     - Validate suspicious user activity and behavior patterns with Customer' Privacy / Compliance Team
     - Implement and monitor a remediation workflow
     - Evaluate outcomes and quantify the value proposition
     - Develop a plan to operationalize and scale the privacy monitoring application across multiple applications and facilities
     - Partner on developing a joint case and publication materials

3. **Implementation Project Scope and Deliverables.**

3.1 **Data Acquisition and Mapping.**

3.1.1 The scope of Verizon Privacy Management is limited to mutually agreeable security / audit log data from a limited set of applications and associated patient and staff demographic data provided by Customer. The source data should be in a mutually agreeable format and include a data dictionary to map required data fields and identify keys across datasets.

3.1.2 Verizon will receive, store, and process the Customer source data within a data center, which complies with HIPAA privacy and security requirements. Verizon will analyze the Customer source data for completeness and accuracy and, with the assistance of Customer Technical Analysts, map the data to the schema.

3.2 **Configuration and Workflow Design.**

3.2.1 Verizon will collaborate with Customer to configure a set of standard health privacy monitoring algorithms utilizing the core privacy monitoring application. As the timeline allows and as necessary, Verizon will work with Customer' Privacy Analysts to tune parameters and run additional iterations to minimize false positives and deliver actionable results.

3.2.2 Verizon will also train Customer Privacy Analysts on the GUI and partner on defining an operational workflow to effectively manage potential privacy violations.

3.3 **Results and Workflow Assessment.**

3.3.1 Verizon will work directly with Customer privacy analysts to validate suspicious user activity and implement a remediation workflow. Verizon will track outcomes of the remediation workflow and summarize the results for Customer virtually or at an appropriate Customer location. The summary will walk through select cases using the privacy monitoring application's GUI to demonstrate how the behavior was identified and the remediation workflow implemented. Verizon also will present static case summaries and analyses in support of the objectives of Verizon Privacy Management.

3.3.2 Additionally, Verizon will develop a framework to quantify the value proposition and solution benefits. As part of this effort, Verizon will collaborate with Customer to develop a plan to operationalize the privacy monitoring application across multiple applications and locations.

3.4 **Deliverables.**

- Online demonstration of select Verizon Privacy Management findings using the privacy monitoring application's GUI.
- Summary of pilot results, including key metadata analysis, algorithms and analytical techniques applied, and significant findings relating the cases and alerts.
- High level framework for benefit quantification and solution architecture design.

4. **Customer's Responsibilities.** Customer is responsible for the following activities in support of Verizon Privacy Management:

- Manage release of data to Verizon through approved processes (e.g. compliant data use agreement, etc.)
- Deliver dataset to Verizon via approved, secure transmission.
- Provide part-time Technical Analyst support for data mapping and testing.
- Provide part-time Privacy Analyst support for role / access policy information, review of preliminary findings, and performance tuning of algorithms.
- Inform Verizon of known data exclusions and previously reported cases of health privacy violations (as appropriate).
- Support integration and analysis of other reference datasets for privacy violation lead generation.
- Collaborate with Verizon to design the operational workflow and remediation planning.
- Provide product feedback on enhancing detection algorithms, GUI, and workflow.
- Partner with Verizon on co-authoring a case study and publication materials.

5. **Implementation Requirements.**

5.1 Each party shall provide a single point of contact and a back-up to the other party who will be the primary interface between such party's internal organizations.

5.2 Each party shall assign a technical resource contact to communicate with the other party regarding the implementation of Verizon Privacy Management including resolution of issues caused by errors in Customer data.

5.3 Each party shall provide knowledgeable personnel familiar with its applications, communications connectivity options and business processes. Such personnel will be expected to provide timely and specific information and data that will be used to assist Verizon in implementing Verizon Privacy Management. Verizon shall be entitled to rely on all information provided by such Customer personnel.

5.4 Each party shall provide the other party with an escalation contact list to be used in the event of issues requiring such party's attention.

Exhibit B
BUSINESS ASSOCIATE AGREEMENT

1. **Customer Agreements Related to Data Security.**

   1.1 **Security Covenants.** Customer hereby agrees that:

   (i) All data that Customer Provides (as defined below) to Verizon was collected by Customer in compliance with all applicable laws, regulations, and directives of all governmental authorities, including but not limited to, all state and federal laws, regulations and directives of the United States, the European Union and its member countries and the countries in the Asia-Pacific region ("Applicable Laws");

   (ii) All data that Customer Provides to Verizon has at all times been stored, transmitted, and otherwise used by Customer in compliance with all Applicable Laws, including, where applicable, the Security Rule promulgated pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") at 45 C.F.R. Part 160 and Subparts A and C of Part 164 (the "Security Rule");

   (iii) All data that Customer Provides to Verizon will be free of viruses and other types of malicious code, errors and unauthorized modifications;

   (iv) Customer will encrypt all data that Customer Provides to Verizon in accordance with industry best practices as endorsed by the National Institute of Standards and Technology; and

   (v) Customer is in compliance with the Security Rule.

   1.2 **Notification.** Customer shall notify Verizon promptly in the event that Customer breaches any of the provisions in Section 1.1 above. Customer shall send such notice to the address for notices as specified in the Agreement

   1.3 **Definition of Provides.** For the purposes of this Section 1, "Provides" means makes available to Verizon in any manner, including, but not limited to, (i) transmits to Verizon; or (ii) stores on Verizon's systems or in its facilities.

2. **Disclaimer.** Verizon will not be liable to Customer or to any third party for, and Customer will be responsible for, any losses, damages, expenses (including reasonable attorneys fees [including allocable costs of in-house counsel] and other legal expenses) resulting from (i) any claim attributable to or arising out of Customer's breach of the covenants contained in this Addendum; and (ii) any claim attributable to or arising out of the misuse, unauthorized access, alteration, theft, destruction, corruption or attacks on or related to the systems and networks of Customer. Nothing set forth in this Section 2 will be deemed to waive or limit the rights or remedies of Verizon under common law or applicable laws, rules, orders or regulations, including without limitation common law indemnity, contribution or impleader.

3. **Privacy Insurance.** Customer shall maintain at least fifteen million dollars ($15,000,000.00) of privacy liability insurance that covers liability arising from the failure by Customer or an independent contractor for whom Customer is legally responsible to properly handle, manage, store, destroy or otherwise control an individual's name, social security number, medical or healthcare data, other protected health information, driver's license number, state identification number, credit card number, debit card number, address, telephone number, account number, account histories, or passwords; and other nonpublic personal information that is the subject of statutes and regulations associated with the control and use of personally identifiable financial, medical or other sensitive information including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and Health Information Technology for Economic and Clinical Health Act; the Gramm-Leach-Bliley Act of 1999; the California Security Breach Notification Act (CA SB 1386) and Massachusetts 201 CMR 17; and other similar state, federal, and foreign identity theft and privacy protection legislation that requires commercial entities that collect personal information to post privacy policies, adopt specific privacy or security controls, or notify individuals in the event that personal information has potentially been compromised. Verizon shall be included as an additional insured under this insurance policy for the aforementioned wrongful acts actually or allegedly committed by Customer or an independent contractor for whom Customer is legally responsible.