QLIK® CUSTOMER BUSINESS ASSOCIATE AGREEMENT

WHEREAS, Customer, either in its capacity as a Covered Entity or a Business Associate (on behalf of a Covered Entity), may provide PHI to Qlik, to act as a Business Associate (either as a 1st or subsequent generation) in the course of Qlik providing the Services to Customer. Pursuant to Customer's obligations as a Covered Entity, and/or the business associate agreements between Customer and its relevant customers, Customer is required under the HIPAA Rules to ensure that Qlik will protect, use and disclose PHI, as set out below, only as necessary to provide the Services, consistent with applicable law and ethical principles, and will appropriately safeguard the PHI. The Parties therefore agree to this BAA as follows:

1. DEFINITIONS

For the purposes of this BAA, all capitalized terms shall have the meaning as defined below as well per the Agreement, and as defined in the HIPAA Rules.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" means the agreement between Qlik and the Customer under which Qlik provides the applicable Services.

"**Business Associate**" shall have the same meaning as the term "business associate" at 45 C.F.R. § 160.103.

"**BAA**" means this Business Associate Agreement.

"**Breach**" shall have the meaning given to the term under the Privacy Rule at 45 CFR § 164.402, in particular the acquisition, access, use, or disclosure of PHI (including Unsecured PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI, including any Security Incident. A Breach shall not include: (i) any unintentional acquisition, access, or use of PHI by a Workforce member or person acting under the authority of Covered Entity, Qlik or Customer, if such acquisition, access, or use was made in good faith and within the scope of authority, and the PHI was not further acquired, accessed, used, or disclosed; (ii) any inadvertent disclosure by a person who is authorized to access PHI at Covered Entity, Qlik or Customer to another person authorized to access PHI at the same entity, or at an organized health care arrangement in which Covered Entity participates, and the information received as a result of such disclosure is not further acquired, accessed, used, or disclosed; or (iii) a disclosure of PHI where Qlik has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information; or (iv) unsuccessful attempts or activities that could not or are not reasonably likely to compromise the security of PHI, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, or (v) events which are caused by the Customer or Customer Affiliates or their end users or third parties operating under their direction, such as the Customer's or Customer Affiliate's failure to (a) control user access; (b) secure or encrypt PHI which the Customer transmits to and from Qlik during performance of the Services; and/or (c) implement security configurations to protect PHI.

"**Client-Managed Deployment**" means a deployment of on-premise Qlik software managed and/or hosted by Customer or by Customer's third-party cloud provider.

"**Consulting Services**" means any consulting services provided to Customer by Qlik pursuant to the Agreement.

"**Covered Entity**" shall have the meaning as the term "covered entity" as under the Privacy Rule at 45 CFR § 160.103 and, for the purposes of this BAA, means either Customer, or Customer's customer for whom Customer is a Business Associate.

"**Data Aggregation**" has the meaning given to that term under the Privacy Rule at 45 CFR § 164.501

"**Designated Record Set**" has the meaning given to that term under the Privacy Rule at 45 CFR § 164.501.

"**DPA**" means the Qlik Data Processing Addendum, if executed by Qlik and Customer according to its terms.

"**Effective Date"** means the date of signature of this BAA by the Parties.

"**Electronic Protected Health Information**" ("**EPHI**") has the meaning given to the term "Electronic Protected Health Information" under the Privacy Rule at 45 CFR § 160.103, limited to the information created, received, maintained, or transmitted by Qlik for or on behalf of the relevant Covered Entity. EPHI is a subset of PHI.

"**HIPAA Rules**" means, as amended from time to time, the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and its associated regulations, and, more specifically, in 45 C.F.R. §§ 160, 162 and 164, *Standards for Privacy of Individually Identifiable Health Information, Final Rule* (the "**Privacy Rule**") and *Health Insurance Reform: Security Standards, Final Rule* (the "**Security Rule**") as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("**HITECH**") and their associated regulations.

"**Individual**" has the meaning given to that term under the Privacy Rule at 45 CFR § 160.103. It also includes a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"**Party**" or "**Parties**" means Qlik and Customer, individually and/or collectively, as the case may be.

"**Protected Health Information**" ("**PHI**") means information (including EPHI) that has the meaning given to the term "Protected Health Information" under the Privacy Rule at 45 CFR §160.103, limited to the information created, received, maintained, or transmitted to Qlik for or on behalf of Customer or Covered Entity. For the avoidance of doubt, PHI does not include (and accordingly this BAA does not apply to) medical/health related personal information not governed by the HIPAA Rules.

"**Qlik**" means the Qlik Affiliate which is party to the Agreement.

"**Qlik Cloud**" means a subscription-based, hosted solution provided and managed by Qlik under the Agreement.

"**Qlik Cloud Customer Content**" means information, data, media, or other content that is uploaded into and residing in Qlik Cloud by Customer or its authorized users on its behalf.

"**Required by Law**" has the meaning given to that term under the Privacy Rule at 45 CFR § 164.103.

"**Secretary**" means the Secretary of the US Department of Health and Human Services.

"**Security Incident**" has the meaning given to that term under the Privacy Rule at 45 CFR § 164.304. For purposes of this BAA, Security Incidents shall not include inconsequential incidents that occur on a frequent basis such as port scans or "pings," and unsuccessful log-on attempts, broadcast attacks on Business Associate's firewall, denials of service or any combination thereof if such incidents are detected and neutralized by Business Associate's anti-virus and other defensive software and not allowed past Business Associate's firewall, or other activities that could not or are not reasonably likely to compromise the security of PHI.

"**Services**" means, pursuant to an Agreement, (i) Qlik Cloud and/or (ii) Support Services and/or Consulting Services requiring Qlik personnel to access or otherwise use PHI to provide Consulting and/or Support Services. Notwithstanding the foregoing, "Services" does not include, and accordingly, this BAA does not cover, (i) Qlik Cloud Customer Content containing PHI which leaves Qlik Cloud, and/or (ii) PHI stored in a Client-Managed Deployment, including but not limited to PHI within self-hosted software.

"**Support Services**" means end user support provided by Qlik to the Customer under the Agreement involving Processing by Qlik of Customer PHI either by way of (i) temporary remote access or screenshare, and/or (ii) receipt by Qlik of Customer files via Qlik's support portal on the Qlik Community website.

"**Subcontractor**" has the meaning given to that term under the Privacy Rule at 45 CFR § 160.103 and, for the purpose of this BAA, means a third-party person or business (including any agents) to whom Qlik delegates a function, activity, or service, and with whom Qlik shares Customer PHI, other than in the capacity of a member of the Workforce of Qlik or a Qlik Affiliate.

"**Termination Date**" means the termination or expiration of the Agreement between the Parties.

"**Unsecured PHI**" means PHI that is not secured through the use of a technology or methodology specified by the Secretary of the United States Department of Health and Human Services (the "Secretary") in guidance issued pursuant to 42 U.S.C. § 17932(h)(2).

"**Workforce**" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Party, is under the direct control of such entity, whether or not they are paid by such entity.

2. USE AND DISCLOSURE OBLIGATIONS OF QLIK

2.1 Use and disclosure. Notwithstanding anything to the contrary in the Agreement, Customer may, pursuant to the terms of this BAA, upload, store or otherwise process PHI in Qlik Cloud. Qlik shall comply with the use and disclosure provisions of the Privacy Rule in performing its obligations under this BAA and the Agreement with Customer and shall not use or disclose PHI other than as permitted or required under this or any other agreement or as Required by Law.

2.2 Other permitted uses and disclosures. Except as otherwise limited and/or provided for in this BAA, Qlik may:

2.2.1 use PHI for the proper management and administration of Qlik or to carry out the legal responsibilities of Qlik;

2.2.2 disclose PHI for the proper management and administration of Qlik, provided that disclosures are Required By Law, or Qlik obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies Qlik of any instances of which it is aware in which the confidentiality of the information has been breached;

2.2.3 use PHI to provide Data Aggregation services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B); and

2.2.4 Qlik may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

2.3 Disclosure documentation. Qlik shall document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Individual's right to receive such accounting under 45 C.F.R. § 164.528. On written request Qlik shall provide to Customer such reasonable information to permit Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Individual's right to receive such accounting under 45 C.F.R. § 164.528.

2.4 Documents requested by Secretary. For purposes of the Secretary determining Customer's (or the relevant Covered Entity, as applicable) compliance with the HIPAA Rules, Qlik shall make available to the Secretary, in a time and manner designated by the Secretary, its internal practices, books, and records (including policies and procedures), relating to the use and disclosure of PHI received from, or created or received by, Qlik on behalf of Customer and/or the relevant Covered Entity.

3. OTHER OBLIGATIONS

3.1 PHI access. Subject to Customer's obligations in Section 4 regarding Qlik Cloud Customer Content, Qlik agrees to provide Customer access, in the time and manner reasonably designated by Customer, to PHI in a Designated Record Set, or, as directed by Customer, to an Individual in order to meet the requirements of 45 C.F.R. § 164.524.

3.2 Amendments to PHI. Subject to Customer's obligations in Section 4 regarding Qlik Cloud Customer Content, Qlik agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity or an Individual, and in the time and manner reasonably designated by the Covered Entity.

3.3 Individual's restriction requests. Subject to Customer's obligations in Section 4 regarding Qlik Cloud Customer Content, Qlik shall comply with an Individual's restriction request, except as otherwise Required by Law, if it is to a health plan for payment or health care operations and pertains to a health care item or service for which the health care provider was paid in full "out of pocket" by the Individual.

3.4 Remuneration for PHI. Qlik acknowledges that it and its Subcontractors are prohibited from directly or indirectly receiving any remuneration in exchange for an Individual's PHI unless the Individual provides a valid authorization pursuant to and in compliance with 45 C.F.R. § 508(a)(4).

3.5 Return and/or destruction of PHI. Except as otherwise provided for in Section 4 relating to Qlik Cloud Customer Content, Qlik shall within a reasonable period of time return or destroy any PHI on the sooner of (a) once the purpose of processing the PHI on behalf of Customer has been fulfilled, or (b) the termination of this BAA. If Qlik destroys such PHI, Qlik shall, upon Customer's written request, certify such destruction in writing. Qlik shall not retain copies of the PHI after termination of the BAA or after the use of such PHI has been fulfilled, other than (i) as part of its data retention and back-up procedures, which shall swiftly delete such PHI shortly after the relevant period, or (ii) as permitted under this BAA. If Qlik reasonably determines that returning or destroying the PHI is infeasible, Qlik shall

provide to Customer notification of the conditions that make return or destruction infeasible. Qlik may retain the PHI that is not feasible to return or destroy, for so long as it remains infeasible to return or destroy such PHI. In such event, Qlik shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Qlik maintains such PHI. The obligations under this Section 3.5 shall survive the termination of this BAA.

3.6 Safeguards and security. Qlik shall implement and use safeguards within its control to prevent use or disclosure of PHI other than as provided by this BAA, which shall include:

3.6.1 implementing and maintaining administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of Customer, and to otherwise comply with the Security Rule in performing Qlik's obligations under this BAA;

3.6.2 mitigating, to the extent practicable, any harmful effect that is known to Qlik of a use or disclosure of PHI by Qlik in violation of the requirements of this BAA;

3.6.3 using reasonable efforts to secure PHI to make it unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance issued under 42 U.S.C. § 17932(h), and any regulation implemented thereunder; and

3.6.4 developing and maintaining policies and procedures to both detect and report Breaches to Customer.

The security details relating to Qlik Cloud may be found in the Qlik Cloud Information Security Addendum found on www.qlik.com.

4. OBLIGATIONS OF CUSTOMER

4.1 Disclosures of PHI. Customer agrees that it will: (i) not make any disclosure of PHI to Qlik if such disclosure would violate the HIPAA Rules or any applicable federal or state law or regulation; and (ii) not request Qlik to use or make any disclosure of PHI in any manner that would not be permissible under the HIPAA Rules or any applicable federal or state law or regulation if such use or disclosure were done by Customer.

4.2 Disclosure of PHI for Consulting Services. Qlik does not require PHI for Consulting Services to be present on Qlik managed systems. In addition to Section 4.1, Customer shall only grant access to PHI to Qlik for Consulting Services, if such access is via a VM/VDI (configured and regulated by the Customer or a third party on their behalf) and if such PHI remains on Customer's systems.

4.3 Disclosure of PHI for Support Services. In addition to Section 4.1, the Parties acknowledge that Qlik does not ordinarily require PHI from a Customer to resolve a technical issue for Support Services. Accordingly:

4.3.1 the Customer shall use their best efforts to minimize any transfer of PHI to Qlik for Support Services. Such efforts shall include but not be limited to removing, or de-identifying PHI in accordance with 45 C.F.R. § 164.514 prior to making it available to Qlik; and

4.3.2 Qlik's total liability in relation to PHI received or accessed by Qlik in connection with Support Services, whether in contract, tort or under any other theory of liability, shall be limited to the previous 12 months' fees paid or payable under the Agreement for Support Services only.

4.4 Notifications. To the extent that such limitation may affect Qlik's use or disclosure of PHI, Customer shall notify Qlik of (i) any relevant limitation(s) in Covered Entity's notice of privacy practices; (ii) any changes in, or revocation of, permission by an Individual to use or disclose PHI; and/or (iii) any relevant restriction to the use or disclosure of PHI to which Covered Entity has agreed and thus Qlik is bound.

4.5 Access and deletion of Qlik Cloud Customer Content during the Agreement. Qlik Cloud is a cloud service with access and deletion of Qlik Cloud Customer Content regulated by Customer; accordingly, Customer is responsible for executing any requests to access, retrieve, correct and delete to Qlik Cloud Customer PHI. Qlik will, as necessary to enable Customer to meet its obligations under HIPAA, provide Customer via availability of Qlik Cloud with the ability to access, retrieve, correct and delete through to the Termination Date its Qlik Cloud Customer Content (including any PHI therein) in Qlik Cloud. The Customer acknowledges that such ability may from time to time be limited due to temporary service outage for maintenance or other updates to Qlik Cloud. To the extent that the Customer, in its fulfilment of its HIPAA obligations, is unable to access, retrieve, correct or delete PHI in Qlik Cloud due to prolonged unavailability (for example, exceeding 10 working days) of Qlik Cloud due to an issue within Qlik's control, upon written request from the Customer, Qlik will where possible use reasonable efforts to provide, correct or delete such PHI. Customer acknowledges that Qlik may maintain backups of Qlik Cloud Customer Content, which would remain in place for approximately thirty (30) days following a deletion in Qlik Cloud. Customer remains solely responsible for the deletion, correction and accuracy of its Qlik Cloud Customer Content and will be solely responsible for retrieving such Qlik Cloud Customer Content to respond to any HIPAA-related request (e.g., from an Individual) relating to PHI within Qlik Cloud Customer Content. If Qlik receives any such request, Qlik will use commercially reasonable efforts to redirect the request to Customer.

4.6 Access and deletion of Qlik Cloud Customer Content on termination of the Agreement. By the Termination Date, the Customer shall delete all Qlik Cloud Customer Content PHI, unless prohibited by law, or the order of a governmental or regulatory body. Notwithstanding the foregoing, after the Termination Date and upon Customer's written request, Qlik will provide reasonable assistance to the Customer to securely destroy or return any remaining PHI within Qlik Cloud Customer Content. Customer acknowledges that PHI may be stored by Qlik after the Termination Date in line with Qlik's data retention rules and back-up procedures until it is eventually deleted. To the extent that any portion of PHI remains in the possession of Qlik following the Termination Date, Qlik's obligations set forth in this BAA shall survive termination of the Agreement with respect to that portion of the PHI, until it is eventually deleted.

4.7 Customer Security Obligations. Customer is responsible for implementing appropriate privacy and security safeguards within its control to protect its PHI. This includes but is not limited to, in relation to Qlik Cloud, Customer (i) configuring and regulating access to Qlik Cloud, (ii) implementing and maintaining adequate logging, and (iii) utilizing customer-managed key ("CMK") functionality. Customer is only authorized by Qlik to input PHI into Qlik Cloud if Customer activates CMK and continues to utilize CMK while its PHI is within Qlik Cloud. Qlik's obligations under this BAA shall not apply in relation to Qlik Cloud if Customer fails to utilize CMK. CMK functionality may not be available for all tenant types and Customer should confirm with their Qlik contact whether their Qlik Cloud tenant has CMK functionality and, consequently, whether they may input PHI into their Qlik Cloud tenant.

5. BREACHES

5.1 Breach notification. Qlik shall, as soon as reasonably practicable and in no event later than ten (10) business days after discovery, report to Customer any use or disclosure of PHI not provided for by this BAA of which it becomes aware, including, but not limited to, any Breach. A Breach shall be treated as discovered as of the first day on which the Breach is known to Qlik or, by exercising reasonable diligence, would have been known to Qlik. The initial notice shall include, to the extent possible, the identification of each Individual whose PHI has been, or is reasonably believed by Qlik to have been, accessed, acquired, or disclosed as a result of such Breach. Qlik shall use its reasonable efforts to collect and provide to Customer as soon as reasonably possible any additional information that Qlik is unable to provide in the initial notice. A notification by Qlik to the Customer of a Breach is not and will not be construed as an acknowledgement by Qlik of any fault or liability of Qlik with respect to the Breach.

5.2 Notification Mechanism. Breach notifications, if any, will be delivered to Customer by any means Qlik selects, including via email. It is the Customer's responsibility to ensure that it provides Qlik with accurate contact information and secure transmission at all times.

5.3 Breach treatment. Qlik shall take reasonable steps to identify, prevent, mitigate and remediate the effects of any Breach. Qlik shall, following notification to Customer of a Breach, cooperate with Customer in providing any and all information accessible to Qlik that is required for Covered Entity to comply with the breach notification provisions of section 13402 of the HITECH and the implementing regulations set forth in Subpart D of the Privacy Rule (45 C.F.R. § 164.400 *et seq*.) and any other applicable breach notification laws and regulations of which Qlik is informed of by Customer.

6. SUBCONTRACTORS

6.1 Use of Subcontractors. Customer acknowledges that Qlik may use Subcontractors in the provision of the Services, as permitted by this BAA and/or the HIPAA Rules.

6.2 Subcontractor Business Associate Agreements. Qlik shall enter into legally binding agreements (i.e., flow-down business associate agreements) with each of its relevant Subcontractors containing fundamentally the same conditions as those contained in this BAA to ensure that any Subcontractor, to whom Qlik provides PHI (received from, or created or received by, Qlik on behalf of Qlik or Covered Entity), agrees to the same restrictions and conditions that apply through this BAA.

7. TERM AND TERMINATION

7.1 Term. The Term of this BAA shall be effective as of the Effective Date and shall automatically terminate on the Termination Date. If it is infeasible to return or destroy the PHI as set out in this BAA, the relevant protections under this BAA shall continue to apply until such PHI is eventually returned or destroyed.

7.2 Termination for cause. Customer may terminate this BAA if there has been a material breach by Qlik of its obligations hereunder. Upon violation of a material term of this BAA by Qlik, Customer may either:

7.2.1 provide a fifteen (15) day opportunity for Qlik to cure the material breach or end the violation. If Qlik does not cure the breach or end the violation within the fifteen (15) day period, Customer may terminate the Agreement and/or this BAA; or

7.2.2 if Qlik has breached a material term of this BAA and cure is not, in Customer's reasonable determination, possible, Customer may immediately terminate the Agreement and this BAA.

8. MISCELLANEOUS

8.1 Scope of this BAA. This BAA shall only apply if, for so long as, and to the extent that, Qlik holds PHI on Customer's behalf. Notwithstanding any other provisions of this BAA, the terms of this BAA shall not alter or diminish the respective responsibilities of Qlik and Customer under the HIPAA Rules, as imposed by operation of law.

8.2 Entire agreement. This BAA contains the entire agreement regarding the subject matter thereof and supersedes any other agreement and communications between the Parties concerning obligations relating to PHI where Qlik is a Business Associate. Except as amended or supplemented by this BAA, the Agreement and any DPA (if applicable) between the Parties will remain in full force and effect. This BAA will govern in relation to PHI, whereas the DPA, if executed according to its instructions and received by Qlik, shall govern with respect to "personal data" as defined thereunder, excluding PHI.

8.3 Amendment. This BAA may not be amended or revised except with the written consent of the Parties. The Parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for the parties to comply with HIPAA, HITECH, the HIPAA Rules and any amendments thereto, and any other relevant federal or state.

8.4 Ambiguities. Any ambiguity in this BAA shall be resolved to permit Customer and Qlik to comply with the requirements of the HIPAA Rules.

8.5 Liability. Subject to Section 4.3.2, the total combined liability of either Party towards the other Party, whether in contract, tort or under any other theory of liability, shall be limited to that set forth in the Agreement as well as any disclaimers contained therein. Any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and this BAA.

8.6 Third Party Rights. This BAA shall not confer any rights or remedies to any other person or entity other than the Parties except as to enable the rights of Individuals if required under the HIPAA Rules. The Parties agree that they are independent contractors and not agents of each other.

8.7 Choice of law. This BAA shall be construed and enforced pursuant to the laws of the jurisdiction set out in the Agreement.

The Parties hereby agree from the Effective Date to be bound by the terms and conditions of this BAA.			
Accepted and agreed to by Qlik		**Accepted and agreed to by Customer**	
Qlik entity	By the Qlik Affiliate which is party to the Agreement	*Customer legal name that is the party to the Agreement (include entity type, e.g., Inc., LLC)*	
Name of signatory		*Name of signatory*	
Position		*Position*	
Signature		*Signature*	
Date		*Date*	