

QBench LIMS Business Associate Addendum

This Business Associate Addendum ("BAA") is entered into between QBench, Inc. ("Company") and the customer agreeing to the terms below ("Customer"), and supplements, amends and is incorporated into the SaaS Services Agreement ("Services Agreement"). This BAA will be effective as of the later date of the two dated signatures below after both parties have signed (the "BAA Effective Date").

Customer must have an existing Services Agreement in place for this BAA to be valid and effective. Together with the Services Agreement, this BAA will govern each party's respective obligations regarding Protected Health Information (defined below).

1. Definitions.

Any capitalized terms used but not otherwise defined in this BAA will have the meaning given to them in HIPAA and the HITECH Act.

"Business Associate" has the definition given to it under HIPAA.

"Breach" has the definition given to it under HIPAA. A Breach will not include an acquisition, access, use, or disclosure of PHI with respect to which Company has determined in accordance with 45 C.F.R. § 164.402 that there is a low probability that the PHI has been compromised.

"Covered Entity" has the definition given to it under HIPAA.

"Covered Functionality" means the data storage, processing, and retrieval functionality of the QBench LIMS product, not including automated emailing functionality or any third-party system that may be connected via API integration with QBench LIMS.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

"Protected Health Information" or "PHI" has the definition given to it under HIPAA and for purposes of this BAA is limited to PHI, including ePHI, within data stored within the QBench LIMS product to which Company has access through the Covered Functionality in connection with Customer's permitted use of Covered Functionality.

"Security Breach" means any Breach of Unsecured PHI or Security Incident of which Company or Customer becomes aware that may be related to Covered Functionality.

2.

"Security Incident" has the definition given to it under HIPAA.

3. **Applicability.**

This BAA applies to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via Covered Functionality and to the extent Company, as a result, is deemed under HIPAA to be acting as a Business Associate or Subcontractor of Customer. Customer acknowledges that this BAA does not apply to, or govern, any other product, service, or feature that is not Covered Functionality.

4. **Use and Disclosure of PHI.**

- a. Except as otherwise stated in this BAA, Company may use and disclose PHI only as permitted or required by the Services Agreement and/or this BAA or as Required by Law.
- b. Company may use and disclose PHI for the proper management and administration of Company's business and to carry out its legal responsibilities, provided that any disclosure of PHI for such purposes may only occur if: (1) required by applicable law; or (2) Company obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Company will be notified of any Security Breach.
- c. Company may also use PHI to create de-identified information in a manner consistent with the standards stated in HIPAA, and may use or disclose such de-identified PHI for any purpose in accordance with HIPAA. Company shall limit its use or disclosure of PHI to the minimum necessary amount in accordance with 42 U.S.C. § 17935(b) and 45 C.F.R. § 164.502(b)(1) or any other guidance issued thereunder.
- d. Company has no obligations under this BAA with respect to any PHI that Customer creates, receives, maintains, or transmits outside of the Covered Functionality (including Customer's use of its offline or on-premise storage tools or any QBench integration) and this BAA will not apply to any PHI created, received, maintained or transmitted outside of the Covered Functionality.

5. **Customer Obligations.**

- a. Customer may only use the Covered Functionality to create, receive, maintain, or transmit PHI. Customer is solely responsible for managing whether Customer's end users are authorized to share, disclose, create, and/or use PHI within the Covered Functionality.
- b. Customer will not request that Company or the Covered Functionality use or disclose PHI in any manner that would not be permissible under HIPAA if done by Customer (if Customer is a Covered Entity) or by the Covered Entity to which Customer is a Business Associate (unless expressly permitted under HIPAA for a Business Associate).
- c. Customer will take appropriate measures to limit its use of PHI to the Covered Functionality and will limit its use within the Covered Functionality to the minimum extent necessary for Customer to carry out its authorized use of such PHI.

Furthermore, Customer shall be responsible for any misuse and action or inaction in connection with use of Covered Functionality.

- d. Customer warrants that it has obtained and will obtain any consents, authorizations and/or other legal permissions required under HIPAA and/or other applicable law for the disclosure of PHI to Company. Customer will notify Company of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Company's use or disclosure of PHI. Customer will not agree to any restriction on the use or disclosure of PHI under 45 CFR § 164.522 that restricts Company's use or disclosure of PHI under the Agreement unless such restriction is required by law.

6. Appropriate Safeguards.

Company and Customer will each use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Functionality.

7. Reporting.

- a. Subject to Section 6(d), Company will promptly notify Customer following Company's Discovery of a Security Breach in accordance with HIPAA and in the most expedient time possible under the circumstances, consistent with the legitimate needs of applicable law enforcement and applicable laws, and no later than seven (7) days after taking any measures Company deems necessary to determine the scope of the Security Breach and to restore affected Company's systems to a reasonable extent.
- b. To the extent practicable, Company will use commercially reasonable efforts to mitigate any further harmful effects of a Security Breach caused by Company.
- c. Company will send any applicable Security Breach notifications to the QBench administrator(s) and/or the contact assigned per the Services Agreement using the email address provided by Customer to Company.
- d. Notwithstanding Section 6(a), this Section 6(d) will be deemed as notice to Customer that Company periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification or destruction of information, or interference with the general operation of Company's information systems and the Covered Functionality. Customer acknowledges and agrees that even if such events constitute a Security Incident as that term is defined under HIPAA, Company will not be required to provide any notice under this BAA regarding such unsuccessful attempts other than this Section 6(d).
- e. Customer shall report any Security Breach to QBench within 20 days of discovery.

8. Subcontractors.

Company will take appropriate measures to ensure that any Subcontractors used by Company to perform its obligations under the Services Agreements that require access to PHI on behalf of Company are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Company uses Subcontractors in its performance of obligations hereunder, Company will remain responsible for their

performance as if performed by Company.

9. Access and Amendment.

Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Covered Functionality, including whether Customer maintains such PHI in a Designated Record Set within the Covered Functionality. Company will provide Customer with access to Customer's PHI via the Covered Functionality so that Customer may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to Designated Record Sets, including rights of access or amendment of PHI. Customer is responsible for managing its use of the Covered Functionality to appropriately respond to such Individual requests.

10. Accounting of Disclosures.

Company will document disclosures of PHI by Company and provide an accounting of such disclosures to Customer no later than thirty (30) days upon receiving a written request from Customer as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA.

11. Access to Records.

To the extent required by law, and subject to applicable attorney client privileges, Company will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created or received by Company on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this BAA.

12. Expiration and Termination.

- a. This BAA will terminate on the earlier of (i) a permitted termination in accordance with Section 11(b) below, or (ii) the expiration or termination of all Services Agreements under which Customer has access to Covered Functionality.
- b. If either party materially breaches this BAA, the non-breaching party may terminate this BAA on 10 days' written notice to the breaching party unless the breach is cured within the 10-day period. If a cure under this Section 11(b) is not reasonably possible, the non-breaching party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section 11(b), the non-breaching party may report the violation to the Secretary, subject to all applicable legal privileges.
- c. If this BAA is terminated earlier than the Services Agreements, Customer may continue to use the Services in accordance with the Services Agreements, but must delete any PHI it maintains in the Covered Functionality and cease to further create, receive, maintain, or transmit such PHI to Company.

13. Return/Destruction of Information.

On termination of the Services Agreements, Company will return or destroy all PHI received from Customer, or created or received by Company on behalf of Customer; provided, however, that if such return or destruction is not feasible, Company will extend the

protections of this BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

14. Miscellaneous.

- a. Survival.** Section 12 (Return/Destruction of Information) will survive termination or expiration of this BAA.
- b. Counterparts.** The parties may execute this BAA in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

15. Effects of Addendum.

To the extent this BAA conflicts with the remainder of the Services Agreement(s), this BAA will govern. This BAA is subject to the governing law clause included in the "Miscellaneous" section in the Services Agreement(s). Except as expressly modified or amended under this BAA, the terms of the Services Agreement(s) remain in full force and effect.