**Company X Vendor Agreement**

***[INSTRUCTIONS (delete before uploading edited form):***

* ***This is a SAMPLE Vendor Agreement. Discuss this with your legal counsel to ensure you make the changes necessary to best fit the requirements of your own organization.***
* ***Delete any “Optional” or highlighted passages that do not apply to the agreement between you and your vendor.***
* ***Modify the “Optional” and highlighted passages you keep to reflect the specifics of your agreement with your vendor.***
* ***Indentations are included to help improved readability. After editing, you may choose to remove indentations, spacing, etc. Make this determination with your legal counsel.***
* ***Delete, or modify appropriately for your organization, highlighted passages before executing the agreement, along with deleting the entire “Introduction” section.]***

**SAMPLE Vendor Agreement**

**Introduction** ***[NOTE: Most organizations can choose to delete this entire Introduction section before using as an actual binding contract. However, some choose to keep it to provide clarification for the purposes of this agreement to those using it. Discuss with your legal counsel to make the best decision for your organization.]***

A “Vendor” is a person or entity, other than a member of the workforce of Company X, who performs functions or activities on behalf of, or provides certain services to, Company X that involve access by the Vendor to personal information and other types of confidential and/or sensitive information.  A “Vendor” also is a subcontractor that creates, receives, maintains, or transmits personal information and other types of confidential and/or sensitive information on behalf of another Vendor.  Many data protection laws and regulations, in the U.S. and throughout the world, generally require that organizations and Vendor enter into contracts with their Vendor to ensure that the Vendor will appropriately safeguard personal information and other types of confidential and/or sensitive information.  The Vendor contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of personal information and other types of confidential and/or sensitive information by the Vendor, based on the relationship between the parties and the activities or services being performed by the Vendor.  A Vendor may use or disclose personal information and other types of confidential and/or sensitive information only as permitted or required by its Vendor contract or as required by law.  A Vendor is generally directly liable under the laws and regulations that apply to the organization for which they are performing business services and subject to civil and, in some cases, criminal penalties for making uses and disclosures of personal information and other types of confidential and/or sensitive information that are not authorized by its contract or required by law. A Vendor also is generally and usually directly liable and subject to civil penalties for failing to safeguard personal information and other types of confidential and/or sensitive information in accordance with the laws and regulations that apply to the organization for which they are performing business services.

A written contract between Company X and a Vendor must:

(1) establish the permitted and required uses and disclosures of personal information and other types of confidential and/or sensitive information by the Vendor;

(2) provide that the Vendor will not use or further disclose the information other than as permitted or required by the contract or as required by law;

(3) require the Vendor to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of applicable data protection laws and regulations with regard to electronic personal information and other types of confidential and/or sensitive information;

(4) require the Vendor to report to Company X any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured personal information and other types of confidential and/or sensitive information;

(5) require the Vendor to disclose personal information and other types of confidential and/or sensitive information as specified in its contract to satisfy Company X’s obligation with respect to individuals' requests for copies of their personal information and other types of confidential and/or sensitive information, as well as make available personal information and other types of confidential and/or sensitive information for amendments (and incorporate any amendments, if required) and accountings;

(6) to the extent the Vendor is to carry out Company X’s data protection obligations under laws and regulations, require the Vendor to comply with the requirements applicable to the obligation;

(7) require the Vendor to make available to Company X, and when applicable any associated regulatory oversight agency, its internal practices, books, and records relating to the use and disclosure of personal information and other types of confidential and/or sensitive information received from, or created or received by the Vendor on behalf of, Company X for purposes of determining compliance with the applicable data protection laws and regulations;

(8) at termination of the contract, if feasible, require the Vendor to return or destroy all personal information and other types of confidential and/or sensitive information received from, or created or received by the Vendor on behalf of, Company X;

(9) require the Vendor to ensure that any subcontractors it may engage on its behalf that will have access to personal information and other types of confidential and/or sensitive information agree to the same restrictions and conditions that apply to the Vendor with respect to such information; and

(10) authorize termination of the contract by Company X if the Vendor violates a material term of the contract.  Contracts between Vendor and other Vendors that are subcontractors are subject to these same requirements.

This document includes sample Vendor agreement provisions to help organizations and Vendor more easily comply with the Vendor contract requirements.  While these sample provisions are written for the purposes of the contract between Company X and its Vendor, the language may be adapted for purposes of the contract between a Vendor and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the laws and regulations that apply to the organization for which they are performing business services.  The language may be changed to more accurately reflect business arrangements between Company X and Vendor, or Vendor and subcontractor.  In addition, these or similar provisions may be incorporated into an agreement for the provision of services between Company X and Vendor, or Vendor and subcontractor, or they may be incorporated into a separate Vendor agreement. These provisions generally address only concepts and requirements set forth in data protection laws, regulations and standards, and alone may not be sufficient to result in a binding contract under local, state or country laws. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract.  Reliance on this sample may not be sufficient for compliance with local, state or country laws, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

**Vendor Agreement Provisions**

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions. Delete this instructional language before finalizing your agreement.

**Definitions**

Catch-all terms [Define each of the following terms as they apply to your organization. Delete those that do not apply.]:

Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Vendor.  “Vendor” shall generally mean an entity contracted to do some type of work that supports the business in some way for an organization. “Vendor” in reference to the party to this agreement, shall mean [Insert Name of Vendor].

(b) Organization.  “Organization” shall generally reference the party to this agreement, and shall mean [Insert Name of Organization].

**Obligations and Activities of Vendor**

Vendor agrees to:

(a) Not use or disclose personal information and other types of confidential and/or sensitive information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with applicable laws, regulations and legal requirements, as communicated by the Organization, with respect to personal information and other types of confidential and/or sensitive information, to prevent use or disclosure of personal information and other types of confidential and/or sensitive information other than as provided for by the Agreement;

(c) Report to Organization any use or disclosure of personal information and other types of confidential and/or sensitive information not provided for by the Agreement of which it becomes aware, including breaches of unsecured personal information and other types of confidential and/or sensitive information as required by applicable legal requirements, within [Put the amount of time within which notice must be provided. Suggested timeframe is 24 hours, except for any specified breaches putting data subjects at immediate risk of harm, which should be reported as soon as possible] and any security incident of which it becomes aware;

[NOTE: The parties may wish to add additional specificity regarding the breach notification obligations of the Vendor, such as a stricter timeframe for the Vendor to report a potential breach to the Organization and/or whether the Vendor will handle breach notifications to individuals (which would typically not be recommended), the applicable regulatory oversight agencies, and potentially the media, on behalf of the Organization. Delete this passage within the brackets before executing this contract.]

(d) If applicable, ensure that any subcontractors that create, receive, maintain, or transmit personal information and other types of confidential and/or sensitive information on behalf of the Vendor agree to the same restrictions, conditions, and requirements that apply to the Vendor with respect to such information;

(e) Make available personal information and other types of confidential and/or sensitive information set to the [Choose either “Organization” or “individual or the individual’s designee”] as necessary to satisfy Organization’s data protection legal obligations, and to meet any of the Organization’s requirements;

[NOTE: The parties may wish to add additional specificity regarding how the Vendor will respond to a request for access that the Vendor receives directly from the individual (such as whether and in what time and manner a Vendor is to provide the requested access or whether the Vendor will forward the individual’s request to the Organization to fulfill) and the timeframe for the Vendor to provide the information to the Organization. Delete this passage within the brackets before executing this contract.]

(f) Make any amendment(s) to personal information and other types of confidential and/or sensitive information as directed or agreed to by the Organization;

[NOTE: The parties may wish to add additional specificity regarding how the Vendor will respond to a request for amendment that the Vendor receives directly from the individual (such as whether and in what time and manner a Vendor is to act on the request for amendment or whether the Vendor will forward the individual’s request to the Organization) and the timeframe for the Vendor to incorporate any amendments to the information in the designated record set.  Delete this passage within the brackets before executing this contract.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “Organization” or “individual”] as necessary to satisfy Organization’s obligations;

[NOTE: The parties may wish to add additional specificity regarding how the Vendor will respond to a request for an accounting of disclosures that the Vendor receives directly from the individual (such as whether and in what time and manner the Vendor is to provide the accounting of disclosures to the individual or whether the Vendor will forward the request to the Organization) and the timeframe for the Vendor to provide information to the Organization. Delete this passage within the brackets before executing this contract.]

(h)  To the extent the Vendor is to carry out one or more of Organization's obligation(s) under applicable legal requirements; and

(i) Make its internal information security and privacy related practices, books, and records available to the Organization, as well as to the applicable regulatory agencies, upon their request, for purposes of determining compliance with the laws and regulations that apply to the organization for which they are performing business services.

**Permitted Uses and Disclosures by Vendor**

(a) Vendor may only use or disclose personal information and other types of confidential and/or sensitive information

[NOTE: Do one of the options below.  Then, delete this passage within the brackets before executing this contract.]

[Option 1 – Provide a specific list of permissible purposes.  Check with your organization’s lawyer to determine what such purposes would be.]

[Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Service Agreement.” Check with your lawyer about this.]

[NOTE: In addition to other permissible purposes, the parties should specify whether the Vendor is authorized to use personal information and other types of confidential and/or sensitive information to de-identify the information in accordance with applicable legal requirements.  The parties also may wish to specify the manner in which the Vendor will de-identify the information and the permitted uses and disclosures by the Vendor of the de-identified information. Delete this passage within the brackets before executing this contract.]

(b) Vendor may use or disclose personal information and other types of confidential and/or sensitive information as required by law.

(c) Vendor agrees to make uses and disclosures and requests for personal information and other types of confidential and/or sensitive information

[NOTE: Do one of the options below.  Then, delete this passage within the brackets before executing this contract.]

[Option 1] consistent with Organization’s minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the Organization’s minimum necessary policies and procedures.]

(d) Vendor may not use or disclose personal information and other types of confidential and/or sensitive information in a manner that would violate applicable legal requirements if done by Organization [NOTE: if the Agreement permits the Vendor to use or disclose personal information and other types of confidential and/or sensitive information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add “, except for the specific uses and disclosures set forth below.”]

(e) [Optional] Vendor may use personal information and other types of confidential and/or sensitive information for the proper management and administration of the Vendor or to carry out the legal responsibilities of the Vendor.

(f) [Optional] Vendor may disclose personal information and other types of confidential and/or sensitive information for the proper management and administration of Vendor or to carry out the legal responsibilities of the Vendor, provided the disclosures are required by law, or Vendor obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Vendor of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Vendor may provide data aggregation services relating to the health care operations of the Organization.

**Provisions for Organization to Inform Vendor of Privacy Practices and Restrictions**

(a) [Optional] Organization shall notify Vendor of any limitation(s) in the notice of privacy practices of Organization under applicable legal requirements, to the extent that such limitation may affect Vendor’s use or disclosure of personal information and other types of confidential and/or sensitive information.

(b) [Optional] Organization shall notify Vendor of any changes in, or revocation of, the permission by an individual to use or disclose his or her personal information and other types of confidential and/or sensitive information, to the extent that such changes may affect Vendor’s use or disclosure of personal information and other types of confidential and/or sensitive information.

(c) [Optional] Organization shall notify Vendor of any restriction on the use or disclosure of personal information and other types of confidential and/or sensitive information that Organization has agreed to or is required to abide by under applicable legal requirements, to the extent that such restriction may affect Vendor’s use or disclosure of personal information and other types of confidential and/or sensitive information.

**Permissible Requests by Organization**

[Optional] Organization shall not request Vendor to use or disclose personal information and other types of confidential and/or sensitive information in any manner that would not be permissible under applicable legal requirements if done by Organization. [Include, as appropriate, an exception if the Vendor will use or disclose personal information and other types of confidential and/or sensitive information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the Vendor.]

**Term and Termination**

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date Organization terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Vendor authorizes termination of this Agreement by Organization, if Organization determines Vendor has violated a material term of the Agreement [and Vendor has not cured the breach or ended the violation within the time specified by Organization].  [Bracketed language may be added if the Organization wishes to provide the Vendor with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Vendor Upon Termination.

[Option 1 – use the clause below if the Vendor is to return or destroy all personal information and other types of confidential and/or sensitive information upon termination of the agreement]

Upon termination of this Agreement for any reason, Vendor shall return to Organization [or, if agreed to by Organization, destroy] all personal information and other types of confidential and/or sensitive information received from Organization, or created, maintained, or received by Vendor on behalf of Organization, that the Vendor still maintains in any form.  Vendor shall retain no copies of the personal information and other types of confidential and/or sensitive information.

[Option 2—use the clause below if the agreement authorizes the Vendor to use or disclose personal information and other types of confidential and/or sensitive information for its own management and administration or to carry out its legal responsibilities and the Vendor needs to retain personal information and other types of confidential and/or sensitive information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, Vendor, with respect to personal information and other types of confidential and/or sensitive information received from Organization, or created, maintained, or received by Vendor on behalf of Organization, shall:

1. Retain only that personal information and other types of confidential and/or sensitive information which is necessary for Vendor to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to Organization [or, if agreed to by Organization, destroy] the remaining personal information and other types of confidential and/or sensitive information that the Vendor still maintains in any form;
3. Continue to use appropriate safeguards and comply with applicable legal requirements with respect to electronic personal information and other types of confidential and/or sensitive information to prevent use or disclosure of the personal information and other types of confidential and/or sensitive information, other than as provided for in this Section, for as long as Vendor retains the personal information and other types of confidential and/or sensitive information;
4. Not use or disclose the personal information and other types of confidential and/or sensitive information retained by Vendor other than for the purposes for which such personal information and other types of confidential and/or sensitive information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under “Permitted Uses and Disclosures By Vendor”] which applied prior to termination; and
5. Return to Organization [or, if agreed to by Organization, destroy] the personal information and other types of confidential and/or sensitive information retained by Vendor when it is no longer needed by Vendor for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the Vendor will transmit the personal information and other types of confidential and/or sensitive information to another Vendor of the Organization at termination, and/or could add terms regarding a Vendor’s obligations to obtain or ensure the destruction of personal information and other types of confidential and/or sensitive information created, received, or maintained by subcontractors.]

(d) Survival.  The obligations of Vendor under this Section shall survive the termination of this Agreement.

**Right to Audit and Perform Risk Assessments** **[Optional, but strongly recommended. Modify this section as appropriate for the contracted activity and organization.]**

1. Organization reserves the right to audit and/or perform a risk assessment on the Vendor and information security controls and processes of any associated Service Providers and to perform relevant tests to ensure that it is compliant with applicable legal requirements for information security and privacy as well as the requirements within this contract.  Vendor will permit the Organization to perform an information security and/or privacy audit and/or risk assessment, including an audit and/or risk assessment of technical, physical and administrative security of any applicable Service Provider premises applicable to the engagement and will cooperate and furnish all requested materials in a timely manner, within no more than [recommend putting “three” here, but use whatever is most appropriate for the business relationship] business days.
2. When requested, Vendor agrees to provide evidence of compliance, such as through an independent information security and/or privacy review or audit commensurate with the requirements of this contract. This audit must be completed within a time frame specified by the Organization.
3. [Optional] Organization will obtain a completed compliance attestation from Vendor executive management each [put “month” or “quarter” depending upon the level of risk with the BA]. Organization will arrange provision of the executive management attestation to the Vendor.
4. [Optional] Organization will obtain [describe any other types of compliance validation requirements here] from the Vendor each [put “month” or “quarter” depending upon the level of risk with the BA].

**Miscellaneous**

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the laws and regulations that apply to the organization for which they are performing business services means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the laws and regulations that apply to the organization for which they are performing business services and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the laws and regulations that apply to the organization for which they are performing business services.

1. No Third Party Beneficiaries. There are no intended third party beneficiaries to this Agreement.
2. Without in anyway limiting the foregoing, it is the parties’ specific intent that nothing contained in this Agreement give rise to any right or cause of action, contractual or otherwise, in or on behalf of any Individual whose personal information is Used or Disclosed pursuant to this Agreement.
3. References. A reference in this Agreement to applicable legal requirements means the data protection laws, regulations or contracts that are in effect or as amended, and for which compliance is required.
4. Amendment. No amendment to this Agreement shall be effective until reduced to writing and signed by the parties. Notwithstanding the foregoing, this Agreement shall be deemed automatically amended to the extent necessary for Organization to continue to comply with the requirements of legal requirements and their implementation, as those requirements may be amended from time to time.
5. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Organization, in the opinion of its counsel, to comply with applicable legal requirements.
6. Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.
7. Authority. The persons signing below have the right and authority to execute this Agreement for their respective entities and no further approvals are necessary to create a binding Agreement.
8. Conflict. In the event of any conflict between the terms and conditions stated within this Agreement and those contained within any other agreement or understanding between the parties, written, oral or implied, the terms of this Agreement shall govern. Without limiting the foregoing, no provision of any other agreement or understanding between the parties limiting the liability of the Vendor to Organization shall apply to the breach of any term, condition or covenant contained in this Agreement by Vendor.
9. Headings. The headings of each section are inserted solely for purposes of convenience and shall not alter the meaning of this Agreement.
10. Governing Law. This Agreement shall be construed in accordance with and governed by the laws of the State of **ENTER THE APPROPRIATE STATE HERE.**

**IN WITNESS WHEREOF,** the parties have executed this Agreement effective upon the effective date set forth above.

 **“Organization”**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Issue Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**“Vendor”**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Issue Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_