Version 1.0

Date: 03/28/19

Vendor Agreement Template

# 1. 0 Purpose

To describe the terms and conditions of your business-to-business relationship as it relates to the privacy and security of the data you share with vendors. It is imperative that your vendor partners protect data according to appropriate laws and regulations. This document is not legal guidance - you should contact an attorney to review and advise on the legal parameters in a formal signed document.

This template uses the word “vendor” as a generic reference to your potential partner; however given the industry in which you operate; vendor may imply “business associate” as defined by HIPAA (Health Insurance Portability and Accountability Act). This document should be amended to reflect the appropriate regulation(s) governing your industry.

# 2.0 Risk Assessment

Organizational risk comprises many types of risk, e.g., management, investment, financial, legal, safety, logistics, supply chain, and security risk. Similarly, security risk has multiple dimensions. Before you enter into an agreement with another organizational entity, you should evaluate the relationship in terms of the data to be shared, its sensitivity and the impact of it either being compromised, damaged, destroyed, or breached. Both parties share the burden and responsibility of the breach. Therefore, it is important to analyze the end-to-end business process with the proposed partner --- what would be the interconnections, the sensitivity of the data to be shared; and dependencies --- before you commit.

Conducting a risk assessment with the proposed partner is a necessary step. Both organizations should clearly delineate the functions, activities, products, and services that comprise the business relationship and flag any risks - such as loss of data, product damage, or schedule slippage. These risks should be identified in advance so appropriate controls and remediation plans be and included in the final vendor agreement.

**3.0 Obligations and Activities of Your Vendor/Business Associate**

While all agreements will be different, there are some common themes that need to be addressed. The following key elements should be included:

A. Data Management - Provide a current data management plan, data recovery plan and incident response plan:

* + What information will your vendor handle;
	+ How will be the data be backed up and recovered;
	+ How will incidents be handled, who will be notified;
	+ How will information be stored;
	+ What is the sensitivity of the data to be stored and shared;
	+ What is the retention period for the data to be stored;
	+ On what platforms will the data be accessed;
	+ Who will have access;
	+ Who is the key point of contact;
	+ How future technology may be deployed;
	+ How will data be destroyed when no longer needed.

B. Disclosure - Provide a statement that the vendor agrees not to use or disclose protected/sensitive identifying information other than as permitted or required by the Agreement or as required by law.

C. Cyber Insurance - Require the vendor to carry cyber liability insurance to cover the costs of: (choose which are applicable):

* + Forensic investigations
	+ Legal advice
	+ Breach notifications
	+ Public relations expenses
	+ Loss of profits from business disruption.

D. Additional Coverage - Require the vendor to cover additional costs associated with a security breach up to [Insert the limitation of liability].

E. Other Provisions - Require the vendor to use appropriate safeguards to prevent use or disclosure of protected/sensitive identifying information other than as provided for by the Agreement, including:

* + Use of encryption
	+ Agreement not to offshore any services related to protected identifying information.

F. Notifications - Require the vendor to report any use or disclosure of protected/sensitive identifying information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected identifying information and any security incident or risk events beyond breach/security incidents (such as loss of material downstream supplier, political risk or labor disputes in a location where key services are performed and IP infringement claims that could

. Include a provision for nondisclosure. Your business associate should not use or disclose protected identifying information other than as permitted or required by the Agreement or as required by law.

3. Cyber Insurance. Consider requiring your business associate to have cyber insurance. There are many helpful conditions these policies should cover (see our cyber insurance page on our website). Policy should include:

* 1. Cost of Forensic investigations
	2. Legal advice fees
	3. Costs to conduct Breach notifications
	4. Costs to cover public relations expenses
	5. Reimbursements for losses incurred due to business disruption

4. Reimbursements. Have a clause that covers reimbursement for additional costs incurred with a security breach up to [Insert the limitation of liability). Items that might include - damage of equipment, loss of data.

5. Use appropriate safeguards to prevent use or disclosure of protected identifying information other than as provided for by the Agreement, including:

* 1. Use of encryption
	2. Agreement not to offshore any services related to protected identifying information

6. Report to covered entity any use or disclosure of protected identifying information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected identifying information and any security incident or risk events beyond breach/security incidents (such as loss of material downstream supplier, political risk or labor disputes in a location where key services are performed, and IP infringement claims that could prohibit use of key technology) of which it becomes aware;

* 1. The Business Associate will report a potential breach to the covered entity [Insert timeframe]
	2. The [Choose Covered Entity or Business Associate] will handle breach notifications to individuals, [Insert applicable government agency], the media and credit monitoring services
1. Ensure than any subcontractors that create, maintain or transmit protected identifying information on behalf of the business associate agree to the same restrictions, conditions and requirements that apply to the business associate with respect to such information;
2. Make available protected identifying information in a designated record set to the [choose either “covered entity” or “individual or the individual’s designees”] as necessary to satisfy covered entity’s obligations;
3. Make any amendment(s) to protected identifying information in a designated record set as directed or agreed to by the covered entity pursuant to [Insert applicable regulation], or to take other measures as necessary to satisfy covered entity’s obligations under [Insert applicable regulation];
4. Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “covered entity” or “individual”] as necessary to satisfy covered entity’s obligations under [Insert applicable regulation];

Date: 03/28/19

Version 1.0

A. Data Management. The vendor is responsible for providing a current data security plan, data recovery plan and incident response plan including:

* 1. What information the business associate/vendor will handle;
	2. How the information will be stored;
	3. The retention period;
	4. On what platforms the data will be accessed;
	5. Who will have access;
	6. Key point of contact;
	7. Accommodation of future technology that may be deployed;
	8. How data will be destroyed or returned when agreement is terminated.

B. Disclosure. The vendor agrees not to use or disclose protected/sensitive identifying information other than as permitted or required by the Agreement or as required by law.

C. Cyber Insurance. The vendor agrees to carry cyber liability insurance covering the costs of:

[Choose all that are applicable]

1. Forensic investigations
2. Legal advice
3. Breach notifications
4. Public relations expenses
5. Loss of profits from business disruption.

D. Additional Costs. The vendor agrees to cover additional costs associated with security breach up to [Insert the limitation of liability].

E. Safeguards. The vendor agrees to use appropriate safeguards to prevent use or disclosure of protected/sensitive identifying information other than as provided for by the Agreement, including:

* 1. Use of encryption
	2. Agreement not to offshore any services related to protected/sensitive identifying information

F. Notifications. The vendor agrees to report to your company any use or disclosure of protected/sensitive identifying information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected identifying information and any security incident or risk events beyond breach/security incidents (such as loss of material downstream supplier, political risk or labor disputes in a location where key services are performed, and IP infringement claims that could prohibit use of key technology) of which it becomes aware;

Vendor Agreement Template

Date: 03/28/19

Version 1.0

* 1. The Vendor/Business Associate will report a potential breach to your company [Insert timeframe];
	2. The [vendor or your company] will handle breach notifications to individuals, [Insert applicable government agency], the media and credit monitoring services. Determine how you want to handle.

G. Subcontractors. Ensure than any subcontractors of the vendor that create, maintain or transmit protected identifying information on behalf of the vendor/business associate agree to the same restrictions, conditions and requirements that apply to the business associate with respect to such information.

H. Designated Record Set. Ensure the vendor agrees to make available protected/sensitive identifying information in a designated record set to your company - name the individual in your company, as necessary to satisfy your regulatory obligations.

I. Accountability. Ensure the vendor maintains and makes available the information required to provide an accounting of disclosures to the [named individual or position in your company] as necessary to satisfy your obligations under [Insert applicable regulation].

**4.0 Permitted Uses and Disclosures by Vendor/Business Associate**

A. Vendors may only use or disclose protected/sensitive identifying information as necessary to perform services set forth in the Vendor Agreement. The vendor is [Choose authorized or not authorized] to perform:

* 1. Data aggregation
	2. De-identification
	3. Combine data with other customer data

B. Vendor may use or disclose protected/sensitive identifying information as required by law;

C. Vendor agrees to make uses, disclosures and requests for protected/sensitive identifying information consistent with your company’s necessary policies and procedures.

Vendor Agreement Template

Date: 03/28/19

Version 1.0

**5.0 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 either party ceases to exist, or your company terminates for cause as authorized in paragraph (5.B) of this Section, whichever is sooner.

B. Termination for Cause. Vendor authorizes termination of the Agreement by your company, if your company determines vendor has violated a material term of the Agreement and has not cured the breach or ended the violation within the time specified; merges with another company, is sold to or acquired by another company, or ceases business operations.

C. Obligations of Vendor Upon Termination. Upon termination of this Agreement for any reason, the Vendor shall [Choose return or destroy] all protected personal identifying information received from your company, or created, maintained, or received by vendor in all forms. Vendor shall retain no copies of the protected/sensitive identifying information.

D. Survival. The obligations of vendor shall survive the termination of this Agreement, unless there is mutual written consent to alternative actions.

# 6.0 References

Much of this vendor agreement language is sourced from the HHS HIPAA link:

<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>

The American Bar Association Cybersecurity Legal Task Force developed a useful checklist that can be used by your team in developing a vendor agreement - here is the full link:

<https://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf>

Vendor Agreement Template