GOSHEN HEALTH HOSTED VENDOR SECURITY QUESTIONNAIRE

As a prospective vendor, or existing vendor hosting Goshen Health or business partner confidential information, you are required to complete our Hosted Vendor Security Questionnaire in order to continue with a business relationship with Goshen Health (referred to as CLIENT through this document).

This questionnaire should be filled out jointly with your organization's Information Security Officer or qualified information security personnel. Please complete the form electronically as printing the form will limit the space for replies. Be sure that the questionnaire is completed in its entirety and that you provide details and attachments as requested and/or necessary.

Please return the completed questionnaire and all requested attachments to the following mailbox: ITSecuritySurvey@GoshenHealth.com.

Further questions may be needed and in some cases a telephone call will be scheduled to verify the answers supplied.

Regards,
Goshen Health Information Security

GOSHEN HEALTH VENDOR CONTACT INFORMATION

Vendor	
Address 1	
Address 2	
City	
State	
Zip/Postal Code	
Country	
Vendor Primary Contact Name	
Vendor Primary Contact Phone Number	

SITE INFORMATION

(Physical location for CLIENT specific business data)

Site Address 1	
Site Address 2	
City	
State	
Zip/Postal Code	
Country	

BUSINESS DESCRIPTION

Please describe the services provided by the Vendor to CLIENT.	
If you do\will connect to CLIENT, how will\do you connect (Site-Site VPN, Internet, etc.)	
Please describe ALL CLIENT applications and access that the Vendor's employees and subcontractors have access to.	

Name(s) of all subcontractors to Vendor listed above:

Vendor Subcontractor Name(s)	Describe responsibilities of Subcontractors to Vendor	Does subcontractor do business outside of the US? (Yes or No)	Does subcontractor access or store CLIENT data outside of the US? (Yes or No) If yes, provide description	If PHI is hosted, a Business Associate Agreement with CLIENT Contracted Vendor is signed? (Yes or No)

List vendor and\or subcontractor handling of CLIENT data: (list vendor name(s) that are applicable next to handling category)

Vendor and Vendor Subcontractors	Create records	Receive records	Maintain records	Transmit records	Responsible for Confidentiality of records	Responsible for Integrity of records	Responsible for Availability of records

Security and Privacy Policies – Domain 1			
Item	**Control**	**Y/N/NA**	**Details**
1.	Does a formal Privacy policy exist?		
a.	If yes, has it been reviewed by a qualified attorney?		
2.	Does your privacy policy allow you to share information with third parties?		
3.	Do you collect, store, maintain or distribute credit card data, protected health information, or personally identifiable information?		
a.	If yes, please provide details.		
4.	Does a formal Information Security Policy exist?		
a.	Describe the Information Security Policy approval process.		
5.	Are Information Security Policies reviewed and updated on a scheduled basis?		
a.	If yes, how often?		

Organizational Security – Domain 2			
Item	**Control**	**Y/N/NA**	**Details**
1.	Is the role of Information Security Officer formally documented?		
2.	Is the Information Security program based upon a formal information security framework or standard such as ISO 17799, ISO 27001, NIST, HITRUST, etc.?		
a.	If yes, which framework or standard is used to protect CLIENT data?		
b.	If yes, how often and by whom is the security compliance program measured?		
c.	If no, are there any plans to have a formal security compliance program in place and by when?		
3.	Describe the organizational reporting structure for Information Security. Please attach any organization charts in support of this query.		
4.	Describe how Information Security functions are managed (i.e., centralized, decentralized)		
5.	Describe the security related credentials of your Information Security Officer.		
6.	Describe the number of FTE's dedicated to your information security program.		
7.	Does your organization have a security strategy?		
8.	Does your organization have a threat intelligence program?		
9.	Has your organization documented its security architecture?		

Asset Classification – Domain 3

Item	Control	Y/N/NA	Details
1.	Has information classification definitions been defined?		
a.	Describe your information classification labels or provide an attachment.		
2.	Does your classification program apply to all forms for information, including paper, disks and data?		
3.	Describe the minimal control requirements for each information classification.		
4.	Do you have a documented process for the review of data access?		
a.	If yes, what is the frequency for reviewing employee access to information?		
5.	Do you have a formal information security risk assessment and management policy?		
a.	If yes, is the information security risk assessment performed internally by a qualified information security person or group separate from the risk owner, conducted externally or both? (Internal Audit is not accepted as their scope is narrow)		
b.	If yes, what is the frequency of this information security risk assessment process?		
c.	If yes, what were the results of the last risk assessment (number of findings and associated risk ratings)?		
6.	Describe the process for data destruction. (General only – policy-based, ad-hoc, regulatory controlled, etc.)		

Personnel Security – Domain 4

Item	Control	Y/N/NA	Details
1.	Are employees required to sign confidentiality/non-disclosure agreements as a condition for employment?		
2.	Are background checks and/or drug testing required as a condition for employment?		
a.	If yes, please describe the types of checks conducted, length of background reviewed and if the employees are allowed in training while the check is conducted.		
3.	Is security supported and championed by executive management?		
4.	Are policies and procedures regarding corporate information security promoted by executive management?		
5.	Does management require personnel to receive security awareness training?		
a.	If yes, does the training provided comply with the government regulations (HIPAA, PCI DSS, etc.) requirements?		
6	Does the Vendor believe they have all the information security requirements needed from CLIENT?		
7.	Is the training conducted at least annually?		

8.	Does management hire personnel against specific job descriptions?		
9.	Do you have a documented incident response process?		
10.	Does your incident response process require notification to your clients?		

Physical and Environmental Security – Domain 5

Item	Control	Y/N/NA	Details
1.	Is access to the production data center limited to those with a business need?		
2.	Is the access to your data center reviewed on a scheduled basis?		
3.	Are physical security policies and procedures adhered to and enforced?		
4.	Do you provide business outsourcing services to CLIENT?		
a.	If yes, do persons with access to CLIENT information maintain a paperless environment?		
b.	If yes, are personal cameras, camera phones, USB drives, etc. allowed in the areas used to support services for CLIENT?		
c.	If no, what other controls are used to reduce the possibility of CLIENT information being misused?		
5.	Is the primary data center that is used by the outsourcing agents in the same physical location?		
a.	If no, please give all data center address location used.		
6.	Are physical asset end-of-life disposition policies and procedures adhered to and enforced?		
7.	Is an auditable, documented inventory of IS assets available in case of loss or theft?		
8.	Are fire suppression mechanisms built into the data center?		
a.	If yes, please describe the suppression used.		
9.	Describe how visitor access to your facility is managed. Please include descriptions of the electronic access controls, video cameras or other supporting security.		
10.	Describe the controls for access to the data center and the location of the data center if separate from the outsource services provided to CLIENT. Please include descriptions of the electronic access controls, video cameras or other supporting security.		

Communications and Operations Management – Domain 6

Application Management

Item	Control	Y/N/NA	Details
1.	Are application and site design objectives documented prior to initiation of development?		
2.	Are business unit owners and executives required to sign off on design requirements?		
3.	Is software used for version control?		
a.	If yes, please describe which software and version.		

4.	Are license management procedures documented and followed?		
5.	Is live code subjected to undocumented development updates?		
6.	Is a change control process and methodology employed?		
7.	Is the project or system used standalone?		
8.	Are production, test, and development environments physically and logically separated?		
9.	Do developers have write access to production code?		
10.	Is load testing completed and approved before any new code is deployed?		
11.	What languages are used in application development?		
12.	Is management required to authorize deployment of new code to production?		
13.	Is any active content used in this application?		
14.	Does this application require the use of a thick client?		
15.	Does this application require the use of a thin client?		
16.	Is software scanned for vulnerabilities and/or improper coding practices?		
Wireless			
Item	**Control**	**Y/N/NA**	**Details**
1.	Do you have a documented policy for wireless technology?		
2.	Is wireless technology deployed within your environment?		
Cryptography			
Item	**Control**	**Y/N/NA**	**Details**
1.	Are policies and procedures regarding encryption key and certificate management in place?		
a.	If yes, are these policies enforced?		
2.	Is sensitive data encrypted during storage?		
3.	Is sensitive data encrypted on backup media?		
4.	Is sensitive data encrypted during transmission on the network?		
5.	Does the e-mail system in use support encryption?		
6.	Are sensitive e-mails required to be encrypted?		
7.	Is TLSv1.2 or higher used for web-based communication of sensitive information?		
Access Control – Domain 7			
Access Control Systems			
Item	**Control**	**Y/N/NA**	**Details**
1.	Are user authentication procedures documented?		
2.	Are policies and procedures related to access control adhered to and enforced?		

3.	Are login banners displayed to ensure users are aware of resource ownership and policies?		
4.	Are all access points into individual computing resources documented?		
5.	Are systems that process and store sensitive data isolated and protected by firewalls?		
6.	Is back-up media isolated and protected?		
7.	Is configuration management used in the technology life cycle process to account for new and existing equipment?		
8.	Can user access be tracked to individuals to provide accountability?		
9.	Is data on computing resources classified and protected to its level of sensitivity?		
10.	Are user access reviews periodically conducted to ensure user privileges are not excessive?		
11.	Are systems monitored to ensure access privileges are not excessive?		
12.	Are employees and vendors bonded?		
13.	Are recertification's periodically performed so that management can verify an individual's need to retain privileges?		
14.	Are data destruction techniques used that are in step with data classification schemes and/or data retention policy?		
15.	Is sensitive information destroyed at the end of its lifecycle?		
16.	Is there a problem management process in place?		
17.	Are deviations from information security standards documented?		
18.	Are deviations from information security standards monitored?		
19.	Are inactive accounts over 90 days old disabled or removed?		

Password			
Item	**Control**	**Y/N/NA**	**Details**
1.	Have password strength, composition and expiration procedures been created that include the following: a) *The length of time between when a password is set and when the password will expire is no more than 90 days* b) *The minimum number of passwords stored in the password history is 24 passwords* c) *The minimum number of days a password must be used is 1 days* d) *Are Initial passwords set by to be expired at first use?* e) *The minimum number of characters for passwords is 12.* f) *Passwords are required to be a mix of numeric, alphabetic, and special characters.* g) *Please attach any supporting documents that describe your password policy.*		

User Management			
Item	**Control**	**Y/N/NA**	**Details**
1.	Are all user accounts and privileges request and reviewed by management or security personnel?		
2.	Are user accounts removed from the system when there is no longer a business need for that account?		
3.	Have network systems been configured to enforce password policies?		
4.	Have generic accounts with administrative privileges been disabled or deleted?		
5.	Are user accounts given the least privilege to complete the business function required?		
Remote Access			
Item	**Control**	**Y/N/NA**	**Details**
1.	Where services are provided to support CLIENT, is remote access to the network allowed?		
2.	Are corporate policies and standards for remote access adhered to and enforced?		
3.	Describe the authentication controls for remote users.		
Application Access			
Item	**Control**	**Y/N/NA**	**Details**
1.	Can the application be configured to enforce varying password policies?		
2.	Does the application support adherence to and enforcement of corporate policies regarding access control?		
3.	Can default accounts be deleted or disabled?		
4.	Can the application be configured to allow for access based on specific roles or functions?		
5.	Does the application store or transmit passwords in clear text?		
6.	Does the application use group IDs or passwords?		
Monitoring System Access			
Item	**Control**	**Y/N/NA**	**Details**
1.	Is Network Intrusion Detection deployed on all critical network segments?		
2.	Is Host Intrusion Detection deployed on all production servers?		
3.	Is Acceptable Use/Data Leakage Monitoring in use?		
a.	If yes, please describe who administrates the monitoring of acceptable use.		
4.	Describe your process for security event monitoring and notification.		
5.	Is an independent 3rd party vulnerability and penetration test conducted on the network and system?		
a.	If yes, how often are these tests conducted and by whom?		
6.	Are internal and remote users monitored for compliance with handling confidential information?		
a.	If yes, please describe methods include technology and process for compliance.		
7.	Do you have a policy and procedure for audit log reviews? If yes, please describe.		

Network Access			
Item	**Control**	**Y/N/NA**	**Details**
1.	Are there network diagrams documenting all entry points into your network?		
a.	If yes, please attach only those diagrams that describe connectivity into your network.		
b.	If yes and this is an outsource provider, provide the data connectivity diagrams from entry into your network to the agent desktop level. Please include how internet connectivity is provided to the agents, including proxies, firewalls and monitoring systems used.		
2.	Are network resources monitored to ensure: a) ***Availability?*** *Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.* b) ***Confidentiality?*** *Assurance that information is shared only among authorized persons or organizations* c) ***Integrity?*** *Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose.*		
3.	Are network change control procedures implemented?		
4.	Are firewalls employed?		
5.	Are firewalls configured to deny all except that which is explicitly allowed?		
6.	Are Virtual Private Networks utilized for secure Business to Business communications?		
7.	Are the following log files reviewed and available for review: *a. Firewalls* *b. Intrusion Detection Systems* *c. VPNS* d. *Hosts*		
8.	Will log files be provided to CLIENT's Information Security group in the event of an incident?		
9.	Are build guides published for various operating systems and followed when building servers?		
10.	Are servers audited prior to deployment to ensure build guidelines have been followed?		
11.	Are services and ports that are open/running limited to those required for business purposes?		
12.	Are servers and network devices regularly scanned to ensure security policies are enforced?		
13.	Do the DNS servers prevent internal, private DNS information from being displayed publicly?		

Business Continuity Planning – Domain 8			
Item	**Control**	**Y/N/NA**	**Details**
1.	Does the data center have a back-up site?		
	If yes, what type?		

	A. ***Hot Site*** *– Hot sites are fully operational facilities providing a predesignated amount of space, equipment, and services at a reasonable cost.* B. ***Warm Site*** *– Warm sites typically refer to an office space or computer center that is equipped with the necessary hardware and communications interfaces.* C. ***Cold Site*** *– Cold sites feature a space set up with a computer system reserved for the subscriber company and intended to support businesses whose disaster recovery needs extend beyond the predetermined period for use of the hot site.* D. ***Mobile Unit*** *– Facilities on wheels that can be transported from one location to another and are equipped with data and voice communications systems.* E. ***Reciprocal Agreements*** *– Companies agree to share their systems with each other in the event that one has a disaster.*		
2.	Is sensitive or mission critical data backed-up on a regular basis?		
3.	Are mission critical systems redundant?		
4.	Are disk configured to be fault tolerant?		
5.	Do contracts or service level agreements include disaster recovery clauses?		
6.	Are disaster recovery plans tested periodically?		
7.	Does the business unit have a business continuity plan?		
8.	Has a business continuity plan coordinator been assigned?		
9.	Who is the contact person for the business continuity plan?		
10.	Have any significant events taken place recently that would cause the plan to be outdated?		
11.	What is the date the plan was last validated or updated?		
12.	Are the backup's stored offsite in a secure location?		
13.	Can you provide a current copy of your disaster recovery plan as it relates to providing services for CLIENT?		
14.	Does the disaster recovery plan have call lists and notification procedures to alert CLIENT of disruptions including off-hour and weekend coverage?		
15.	Are the Vendor call lists synchronized with the CLIENT contacts and notification procedures?		
16.	Has there been an event (e.g. weather, cable cuts, strikes, etc.) in the past 12 months that has caused your service to CLIENT to be interrupted?		
a.	If yes, please describe each event.		
b.	If yes, please describe what controls were implemented to prevent further interruption.		
17.	Have you specified information that is needed from CLIENT to respond and adequately provide support during an event?		
18.	Does the disaster recovery plan contain information as to how the Vendor stages their response including people, equipment, and recovery locations?		

19.	Is there a regular maintenance and testing schedule for the Vendor's disaster recovery plan?		
20.	Has the disaster recovery plan been tested at least annually?		
21.	Has the Vendor participated in an annual test with CLIENT Holdings?		
22.	Have the results of the Vendor's most recent test been shared with CLIENT?		
a.	If yes, when and by whom?		
23.	Do the Vendor's suppliers have service level and recovery agreements in place to ensure continued support to CLIENT Holdings during an event?		
24.	Does the Vendor have manual workarounds to continue their services if the Vendor suffers a loss of its Information Technology area?		

Law, Investigation and Ethics – Domain 9

Item	Control	Y/N/NA	Details
1.	Are there regulatory agencies regulating this Vendor's working environment?		
a.	If yes, please describe the privacy\security regulations that Vendor must comply with. (e.g. HIPAA, PCI DSS, ePrescribing, State Privacy Laws, 42 CFR2, etc.)		
2.	Has a SSAE 16 SOC2 or 3, or third party inspection been performed on the data center or ASP provider?		
a.	If yes, please attach your organizations SSAE16 SOC2 or 3 report, as well as any subcontractors involved in CLIENT hosting.		
3.	Are all of the applications or systems that CLIENT Holdings uses or interfaces with owned by the Vendor?		
4.	Is there an anonymous reporting function that allows employees or contractors to report suspected fraud or security abuse?		
5.	Have there been any fraud or security issues reported or found by management over the previous 18-month period with respect to services provided to CLIENT?		
a.	If yes, please describe the issues in detail, including how the issues were resolved and controls implemented.		
6.	Are sub-contractors required to provide evidence of insurance?		
7.	Are sub-contractors required to sign non-disclosure agreements that comply with the Vendor's non-disclosure agreement with CLIENT?		
a.	If yes, please describe the types and limits required of your sub-contractors.		
8.	Do you create, manage or have access to detailed credit card information or personal information via CLIENT applications?		
a.	If yes, please describe what access is in place and the description of the data in question.		
9.	Is customer data retained after use?		

10.	Have you been made aware of CLIENT requirements to protect customer information?		
11.	Are you PCI DSS compliant?		
12.	What level and how is this certified?		
13.	When was the last certification? Please provide letter of compliance if conducted by an external 3rd party (QSA).		

Security Architecture and Models – Domain 10

Item	Control	Y/N/NA	Details
1.	Are databases configured to dynamically detect and correct errors?		
a.	If yes, what are the normal databases in use? (e.g. Oracle 10, MySQL, etc.)		
2.	Has the operating system been hardened and all current patches applied?		
a.	If yes and this is an outsource provider, what is the normal operating system/patch level used by servers and desktops in support of access by the provider?		
3.	Is there a process or system in place to manage operating system and application vulnerabilities and their associated patches?		
4.	Are CGI and other active content only configured on hosts that require it?		
5.	Are all hosts and network devices updated with patches and security fixes in a timely manner?		
6.	Is a commercial anti-virus application required on all desktops?		
a.	If yes, please describe.		
7.	Are desktops used in support of access to CLIENT applications hardened?		
a.	If yes, is the print screen disabled?		
b.	If yes, are USB storage devices disabled?		
c.	If yes, is email or IM limited only to supervisors and above?		
d.	If yes, but email and IM is used, please describe the use?		
e.	If yes, is access to the internet limited to only sites allowed by CLIENT vendor management?		
f.	If yes and internet access is limited, please describe the controls in place to limit the access?		
8.	Are system critical files protected by intrusion detection systems?		
9.	Is SSH (Secure Shell) or other forms of strong encryption enabled on all hosts that require it?		
10.	Beyond passwords, are other forms of user authentication used within the Vendor environment that provides strong authentication (e.g., 2-Factor)?		
a.	If yes, please describe.		
11.	Do system administrators have individually assigned login IDs with administrative privileges?		
12.	Are system administrators the only people who have administrative privileges?		

13.	Do Partners, vendors, or services providers require remote access to the Vendor's environment that supports access to CLIENT?		
a.	If yes, please describe.		
14	Do you record telephone calls between your agents/staff and CLIENT customers?		
a.	If yes: What call recording system do you use?		
	If yes: How do you deal with sensitive financial data, i.e. Credit Card Number, CVV2, Checking account number within the audio file?		

Cyber Liability – Domain 11

Item	Control	Y/N/NA	Details
1.	Does your insurance program cover Privacy Liability and provide specific limit?		
2.	Does your insurance program cover Security Liability and provide specific limit?		
3.	Does your insurance program cover Cyber Extortion and provide specific limit?		
4.	Does your insurance program cover Customer Notification Expense and provide specific limit?		
5.	Does your insurance program cover Computer and Legal Forensic Expense and provide specific limit?		
6.	Does your insurance program cover Credit and Identity Repair and provide specific limit?		
7.	Does your insurance program cover Credit and Identity Repair and provide specific limit?		
8.	Does your insurance program cover Business Interruption and Data Recovery Extra Expense and provide specific limit?		
9.	Does your insurance program cover Regulatory Defense and Penalty Coverage and provide specific limit?		
10.	Can you add Goshen Health, Inc. as an Additional Insured on a Primary and Non-Contributory basis?		
11.	What is your Cyber Liability policy per claim and aggregate limit?		

The signatory below should have authority under the Agreement between CLIENT and the Vendor to provide this information.

Vendor: _____

Authorized Representative: _____

Title: _____

Date: _____