

Vendor Questionnaire

Instructions: This questionnaire was developed to assess the vendor’s information security practices and standards. Please complete this form as completely as possible, answering yes or no, and explaining the answer fully.

I. Authentication/Authorization

Question	Yes/No	Full Answer/Comments
1) Is your application integrated or can it be integrated with Hospital’s Central Identity Management Model for both authentication and authorization?	YES	Our compliance delivery system was developed by the team responsible for developing the SafetySend, Inc. compliance messaging system. It is a mature compliance gateway used by organizations such as The United Nations, Tenet Health Systems and other hospitals, universities and government agencies. Based on this level of enterprise integration it would be logical to conclude it would work in an enterprise healthcare provider organization. *If required we will have changes made to accommodate.
a) Do you allow third party integration to your security repository?	YES	If all appropriate security measures, access rights and policy enforcement is in place.
i) Do you have an API set for your security tables?	YES	Available upon request. May require customization for specific applications.
ii) Are roles, facilities, user ID, and password information exposed in the API set?	NO	
iii) What methods do you use for standard integrations? (i.e. Active Directory, LDAP, SAML, etc.)		SafetySend is a versatile technology platform that can handle multiple connections/gateways. We can modify the connections per facility security policy and protocols.
b) What is required from a user to authenticate? (e.g. user ID, password)		USER ID and Password. However for HIPAA/GLBA regulatory compliance practices to be met we store a secondary password and challenge question/answer for additional verification purposes and password reset requests.
2) Do you have role-based security (i.e. access to specific components is based on the role of the user, a Nurse role has x, x, and x capabilities in the system)?	Yes	
3) Will Hospital Intranets be the only method for users accessing this application?	No	We have a SSL VPN intranet/extranet/internet application that can be provided to review patient inquiry information and health history forms.
a) If web-based, is there another URL available outside of the portal?	No	
b) If an outside URL is allowed, is the user authenticated through the IAM?	YES/NO	Depending on security access policy and permission settings.

Vendor Questionnaire

4) Does your application comply with Hospital's standard user ID/password policies?	YES	
a) 8 character strong password?	YES	6-x, any mix of chars
b) firstname.lastname user ID?	YES	Email address
c) password changes at 90 days?	YES	Forced password changes at "X" days per Hospital policy.
d) lockout after 5 invalid logon attempts	YES	Lock out after "X" attempts per Hospital policy
e) cannot use last 5 passwords	YES	Default currently at 3, but change to 5 is acceptable per Hospital policy.
f) Does your application require two-factor authentication? (not required)	YES	We have multiple authentication methods that include: IP, user/pass, Public/Private Key, Port Assignment, etc.
5) Does your application use Hospital's 9-digit unique ID to uniquely identify users?	NO	No provision provided. But we are willing to adopt this into our security policy for Hospital if given specifications.
a) If not, what is used?		Email Address/User ID, Password
b) What specific user information is used as the primary key for users?		Email Address/User ID, Password and security challenges specified in HIPAA §164.306 and GLBA §314.4/5.501
6) Is user credential information ever passed over the internet for authentication or authorization?	YES	
a) If yes, how it is protected (e.g. SSL, other encryption method)?		SSL 256 bit is default but other methods are available upon request.
b) If no, is the user information transmitted within the Hospital environment, and if so, is all transfer of this information behind the firewall within the trusted network?		

II. Audit/ Logging

Question	Yes/No	Full Answer/Comments
1) Is your application subject to SOx, HIPAA, PCI, CMS, or other regulations?	YES	We have been a compliance provider for 8 years.
a) Does your application contain financial data? Can financials be altered or are they view only?	YES	All data in this application is "view only".
b) Does your application contain PHI? If yes, is access secured by facility?	YES	Yes. All data access meets HIPAA and GLBA regulatory compliance standards.

Vendor Questionnaire

c) Does your application take in or store credit card numbers?	YES	But this will not be part of the application as it applies to Hospital in the current form.
2) Does your application produce audit logs?	YES	Our application provides both individual and corporate audit trails as defined in HIPAA and GLBA regulations.
a) In what format?		MS SQL 2005 exported to desired format
b) What fields are tracked and what information is logged about the user interacting with the fields?		Originator of PHI, Recipient of PHI, Time/Date Stamp of Send and Receive, CC, BCC, Expiration Date, Retraction Notification, Retracted by
c) Is this information tracked whenever a record is accessed, when changes are made, or other (explain)?	YES	This information is tracked in "real time" for all individual users. Each individual field has the option of turning tracking on/off per access policy.
d) For ASP, how long is this information stored?		At least 7 years
e) Where/how is this information stored (e.g. centrally, encrypted, trusted network)?		Stored on SAN at primary data center. Carrier grade secure hosting facility with military card key access requirements. Fail over connections to redundant secondary secure facility as well as redundant NAS connection synchronizing daily using encrypted channel.
3) Does your application track logon, logoff, and password resets?	YES	
a) If no, can this be accomplished technically through a web service call or FTP post?	YES	
b) If no, is this information stored within the application, and if so – how and in what format?	YES	SQL
4) Do you store SSN, DOB, passwords, or password security questions/answers for users?	YES	
a) If yes, is this information transmitted to other applications and within the trusted network or outside?	YES	
b) If yes, is the information encrypted during transfer? What encryption method is used?		SSL 1024 bit (scalable upon request)
c) If yes, is this information encrypted at rest? What encryption method is used?		MS SQL 2008 Database Encryption by passphrase
5) Are any processes in place to detect anomalies in user interaction based on business rules, such as one user logged on at multiple locations, large number of invalid logon attempts, etc and are	YES	Multiple Layers. 1. Firewall 2. Proprietary "Interceptor" Application, 3. Web Application and 4. Database Access. Lockout and Denial of Service set per security policy.

Vendor Questionnaire

these processes for follow-up?		Also each user connected to our SSL VPN has individual signature session to prevent "sniffing" data packets.
a) Can these anomalies be detected automatically and trigger events based on pre-determined rules (e.g. alerts, emails, pages, etc)?	YES	Alerts can be sent via email, fax, SMS or recorded voice message.
b) What methods can be used for reporting on logged data?		SQL Dump to CSV, XLS, PDF, etc. in specified format or web access reporting. SharePoint is also an acceptable option
c) Is there a standard reporting mechanism and using what tools?		Yes, Web based reports querying SQL tables
6) Are procedures in place for the following:		
a) Development of application updates and patches?	YES	Specifications must be submitted in writing and approved by both parties
b) Code reviews to ensure data integrity and security?	YES	We have an online support ticket for 24/7/365 support. Code reviews can be done quarterly or as needed to optimize business process.
c) Timely application of patches in the production deployment?	YES	System undergoes daily maintenance routine. All system and security updates are tested on development servers before be applied to production servers.
d) Testing before deployed to production environment?	YES	See above. We are a 8 year old company and product with a mature software development cycle.

III. Threat Evaluation and Response

Question	Yes/No	Full Answer/Comments
1) Are service accounts required for your application to run? If so, how many/what type?	NO	
a) Have you completed an exception for setup and use of these IDs?	YES	All users who are granted access will be given a link to setup their IDs and an administration console will be provided. It is Hospital's responsibility to assign a "security officer" who will have the ability to add/delete users, suspend access, reset passwords, change security questions, modify contact information, etc.
b) For vendor products – how will you connect to your application for support?		There is an integrated support system that is "ticket" based. User will be assigned a support ticket and will have access to review that status of each request. Most support tickets are handled same day with a few handled during system maintenance and will be completed the following day.
c) Is a site-to-site VPN tunnel setup to allow	YES	This can be made available, but not required as a SSL VPN is already

Vendor Questionnaire

secure access?		established.
2) Has your application been scanned for vulnerabilities?	YES	
a) Were the vulnerabilities all remedied?	YES	
b) What tool was used for scanning?		Nessus and Comodo
c) For vendor applications, does your product have any known vulnerabilities?	NO	None that we are aware
3) For ASP models, what is your ongoing vulnerability management process?		Ongoing Vulnerability Scanning, Server Hardening Procedures, Application Hardening Procedures. Our application is locked down pretty tight. We only allow assigned IPs any latitude whatsoever.
a) What scanning mechanism do you use for vulnerability assessment? How often do you scan? What is your process for remediation for vulnerabilities you find?	Nessus	We scan bi-weekly. We take action dependent on the level of vulnerability uncovered. Action could be immediate to during regular scheduled maintenance depending on circumstances.
b) What Anti-virus program do you use? What is the update/patch process? How often are patches pushed?	Multi-Layer	We use a three tiered security process. Firewall uses "Gateway Anti-Virus and Content Filtering" We have an "Interceptor" solution that uses F-Prot for Windows to filter all inbound data traffic and we use a Symantec hybrid solution on our servers.
c) Do you utilize any other software, such as Intrusion Prevention (Network and/or Host), Intrusion Detection, Network Access Control, etc) and if so, using what products?	YES	We have firewall based intrusion detection as well as internal security protocols developed within the application that are "trigger" enabled. We use a SonicWall Pro Firewall for the network segment this web application resides.
4) Has your site undergone a SAS70 audit?	NO	
a) When was the last audit?		
b) What were the results?		
c) How often are these audits performed?		
d) Are you certified under any other standards around information security, such as ISO?	NO	
5) What is your process for notifying customers of potential information breaches?		We have a security officer alert system of scheduled maintenance times, heightened security events and natural disaster events. We have withstood several hurricanes, severe security threats and continue to be stable and trusted solution.
a) What criteria must be met for you to disclose a potential breach?		Network administrators are notified of any potential security breach that is relevant to their "domain" or users immediately. 99.999% of attempts are stopped at firewall level and security officer is not notified. We notify security officer of after multiple failed login attempts, suspicious activity

Vendor Questionnaire

		such as high bandwidth consumption or ANY "unauthorized" access that comes to the attention of network administrators. We provide the ability of a Hospital Security Officer to monitor log in times, IP's and other criteria as needed as a secondary layer of access supervision.
b) How and when is disclosure done?		Security notifications are sent out immediately via emails. SMS, Fax and Recorded Voice Notifications are also available.

IV. Physical Security

Question	Yes/No	Full Answer/Comments
1) Do you employ the following at your data center:		
a) Electronic locks on server room doors?	YES	As well as locked server cabinets inside locked server room doors
b) Access card or biometric readers?	YES	Access Cards
2) Are visitors required to sign in before they have access to the data center?	YES	No visitors allowed who are not on the approved list.
3) Are all doors (offices, storage rooms, etc.) within or near the data center locked at the close of business hours?	YES	Sever room is concrete doors, walls, floors with no additional access points.
4) Is the data center staffed continuously (24/7)? If not, what are the hours of operation?	YES	