McLaren Health Care
Vendor Security Survey

	Information Security Survey	Vendor Responses
	This questionnaire is required for all systems that interact with the company network. *Based on these responses, further discussion and/or technical review may be required.* *Please indicate N/A where necessary; blank responses may cause a delay in processing.*	
	I. Profile Information	
1	Company Name Application name	
2	Brief description of application functionality / high-level overview	
3	Application contact information	Name: Phone: Email:
4	Brief description of application architecture (i.e. ASP, company hosted, web tiers, etc.)	
5	Has your organization achieved HITRUST Validated or Certified status?	
6	Does your company carry cyberliability insurance? If yes, enter coverage limits.	
	General and Off-shore Services	
7	Does your organization store any data off-shore or have any employees working in off-shore components, or off-shore subcontractors or agents with access to servers or information systems which create or process PHI or other data on our behalf?	
8	Does your system contain or transmit electronic Protected Health Information (ePHI) or financial data?	
9	Is your system hosted on the company network or hosted using a Software as a Service (SaaS) model? Please note that all questions must be completed regardless of the hosting model.	
10	Is your system new to the company environment or part of an existing system?	
11	How does your system secure data both in transit and at rest? Please indicate specific protocols and encryption levels (i.e. SSL, VPN, AES 256-bit, etc.).	
	Password Management	
12	Can the system enforce password complexities as outlined in the company password policy? i.e. minimum 7 character length and a combination of alphanumeric characters?	
13	Can the user change their password at any time?	
14	Can the system force periodic password changes and password change at next login?	
15	Does the system support password history to prevent password reuse?	
	Authentication, Authorization, & Access Management	
16	How many users will use the system?	
17	Does the system support role based, user based, or rule based access? Please explain.	
18	Who is responsible for creating new users and how are accounts removed or disabled?	
19	Does your application support integration with company's Active Directory environment?	
20	Does the system support locking out user accounts after a predefined number of failed login attempts?	
21	Can the application be set to automatically log a user off after a period of inactivity (e.g. 15 minutes)?	
22	Describe your organization's licensing model	
	Network & Remote Access	

McLaren Health Care
Vendor Security Survey

23	Has a report on controls, such as an SSAE 16 or a SAS 70, been obtained from the hosting provider? Please provide a copy for review.	
24	Please provide the estimated number of third parties that have access to your network (VPN, SFTP, etc.)	
25	What tools and technologies are used to monitor third party access to your network? How is this validated?	
26	Please provide an architecture document that includes a full network diagram of the application environment, illustrating the relationship between the environment and any other relevant networks.	
27	Please provide network bandwidth requirements. What metrics and benchmarks are available to validate?	
28	Is the application isolated on the host system(s), including a separate infrastructure?	
29	Describe your wireless security model, what encryption and authentication mechanisms are used to protect wireless communications in your environment (e.g. WPA2)	
30	How does your organization assess the security of third party business associates or partners?	
31	What network protocols are required for this application?	
32	Please describe your remote support model. Are individual user accounts assigned to support personnel?	
	Compliance, Incident, and Breach Response	
33	Has your organization had a 'material' security breach within the last 3 years? A ‘material’ security breach includes, but is not limited to, hackers, computer viruses, malicious or unauthorized intrusions to software, network, or physical infrastructure.	
34	Does your organization allow the use of unencrypted portable media (e.g. USB drives, CD's, etc.). How are these media secured?	
35	Are laptops encrypted in your organization? Can laptops potentially contain ePHI or financial data? If so, are the laptops encrypted?	
36	Who in your organization is responsible for managing your external breach notification?	
	Audit & Reporting	
37	What level of auditing does the system support? At the system-, file-, application- record-level? Printing?	
38	Does the system have the capability to audit each time a record is modified *and* viewed containing ePHI, including but not limited to patient demographics?	
39	Please identify the location and format of log files. company requires that audit logs be available for integration with the organization's centralized log management tool.	
	Vulnerability Management	
40	What antivirus and endpoint security solutions are deployed in your environment?	
41	Do you support your system being protected by customer installed antivirus software (Symantec)?	
42	Please provide the date of the last security vulnerability scan run in your environment.	
43	How does your organization stay current with security vulnerabilities and patching?	
44	Please provide the date of the last comprehensive a*ttack and penetration* test in your environment.	
45	Does your organization perform a security code review prior to releasing functionality into Production?	
46	How does your system support secure upload and download utilities?	
47	How are host systems hardened (secured) against attacks? Provide documentation where available.	
48	Does your system require administrative user privileges or access to local hard-drive?	
	Physical Security	

McLaren Health Care
Vendor Security Survey

49	Is the equipment that hosts the application located in a physically secure facility, which requires badge access at a minimum?	
50	Do your media sanitation procedures require secure destruction of electronic and hard copy media?	
51	Will any non-company owned hardware be installed and removed during implementation?	
	Infrastructure and Technical Standards	
52	What operating systems are supported for your application (i.e. Windows 7, Windows Server 2003/2008, Windows XP, AIX , SunOS, Unix, Linux, etc.)	
53	Does your system have any conflicts with Internet Explorer (version 6, 8 or higher)?	
54	Do you support your application running on VMware version 4.0 or higher?	
55	Does your application require dedicated servers and if so provide justification.	
56	Does your system support interfaces to the company's existing clinical and financial systems using industry standard protocols and standards (including HL7, XML, IHE and CCOW).	
57	Does your system support publishing via Citrix?	
58	Does your system require any specialty hardware or appliances to be implemented in company's environment (i.e. peripheral devices, etc.)?	
59	Does your application require Java, if so what version?	
60	Please describe the application footprint (client size, disk space, memory, network bandwidth, etc)	
61	Please outline the minimum workstation requirements for your application (i.e. Operating Systems, RAM, hard disk, etc.)	
	Storage & Availability	
62	What database system and version, if any, is used to support you application/system? (i.e. SQL 2005, Oracle, MySQL, MS Access, etc.). Are databases supported in a shared/clustered environment?	
63	What is your process for monitoring the integrity and availability of the host where the company application will reside?	
64	What functions or options are available to increase the fault tolerance/high availability of your system?	
65	Please describe your organization's Backup and Recovery process.	
66	Please describe data retention practices including how often data is purged.	
	Implementation & Change Management	
67	Please describe your organization's Change Management methodology. Does you organization follow the ITIL standards for Change Management processes?	
68	Do your upgrade and patch processes support the installation and testing in a non-production area prior to implementing in production?	
69	Are the non-production areas completely segregated from the production area?	
70	Please describe the schedule and timing of new version releases and upgrades.	