[LOGO HERE]

HOSPITAL ABC

This questionnaire is to be completed by the company and will be used by Hospital ABC to review security controls for new and partner systems. Please complete the form below and return to:

Privacy/Security Officer

1. Description	
Company Name:	**System Name:**
Company Contact Person/Email/Telephone#:	**Hospital Contact Person/Department:**
Service or function provided by Company on behalf of Hospital: _____	
2. System	
System Description:	
Operating System:	**Application/Database:**
Web-based Application: **Is this a web-based application? ☐ Yes ☐ No** **If Yes:** • **Can access to the web-based application be restricted to a specific range of IP addresses? ☐ Yes ☐ No**	

3. System Location and Support		
☐ **Hospital** ☐ **Clinics, specify:** ☐ **Other, specify:** ☐ **Offsite/Hosted**	**System managed and secured by:** ☐ **Hospital** ☐ **Company** ☐ **Shared responsibility** **Support via: ☐ VPN ☐ Other**	**Support Available:** ☐ **24/7/365** ☐ **Specify hours: _____** _____

4. Data Classification
☐ **Public ☐ Sensitive (internal) ☐ Restricted (protected by law/contract)** **For sensitive or restricted data check all that apply:** ☐ **Patient (ePHI)** ☐ **Credit card (PCI)** ☐ **Personal identifiers (SSN, I-90, etc.)** ☐ **Financial** ☐ **Research** ☐ **Student** ☐ **Other, specify:**
5. Data Transmission and Storage

Is data transmitted to/from this system and other systems? ☐ Yes ☐ No

If Yes:

- **What purpose is the data used for? _____**
  _____
- **How often is data transmitted? ☐Real-time ☐Batch**
- **Where is the data transmitted to? _____**
- **What method is used for data transfer? Include type of encryption. _____**
  _____
- **Does the system/application generate external files, such as test results or discharge summary, in PDF or other format that is stored outside of a database or application? ☐Yes ☐No**
  If Yes, where are the files stored, and how are they protected? _____
  _____

Is data stored in encrypted format (includes all mobile devices)? ☐ Yes ☐ No

- **If yes, describe type of encryption: _____**
  _____

Is data stored, transmitted and/or services provided per cloud computing? ☐ Yes ☐ No

If yes:

- **What is the name of the Cloud Provider(s)? _____**
  _____
- **Is the Cloud Provider located in the United States? ☐ Yes ☐ No**
- **Is there a BAA in place with the Cloud Provider? ☐ Yes ☐ No**

6. Authentication and Authorization

Does the system use Active Directory/LDAP authentication? ☐ Yes ☐ No

If not, what authentication method is used? Please describe.

☐ Simple password or PIN ☐ Complex password/passphrase ☐ Token ☐ PKI/Certificate ☐ Biometric ☐ Other ☐ None

How are user privileges assigned?

☐ Manual selection ☐ Group membership ☐ Role-based access ☐ Access is the same for all users

If the company's employees/contractors will have access to Hospital's systems, list the contact information of the person who will be responsible for notifying the IT Department to deactivate users that are no longer employed by the company:

Name and title: _____

Email address: _____Phone number:_____

The IT Department may be reached at [insert phone] or [insert email].

7. Policies, Procedures, and Controls

Check all documented policies and procedures for the offsite/hosted system:

☐ Security incident response plan ☐ Breach notification procedure ☐ Disaster recovery plan ☐ Business continuity plan

☐ Log management ☐ Risk assessment ☐ System hardening procedure ☐ Antivirus

☐ Patch management ☐ Change management ☐ System backup/restore

Note: Hospital may request copies of documentation.

Check all security controls for the offsite/hosted system:

☐ Network firewall ☐ Host-based firewall ☐ Intrusion prevention ☐ Redundancy ☐ System backup

☐ Antivirus ☐ Patch management ☐ Audit log ☐ Secure disposal ☐ Facility/environment security

☐ Other, please describe: _____

8. Other

Do any of your employees work from home? ☐ Yes ☐ No

If yes, please describe what security measures are in place to assure the home environment is secure:

_____

_____

Describe how you dispose of protected health information – electronic and paper:

_____

_____

Do you have encrypted email? ☐ Yes ☐ No

Comments Section

Use the space below to provide any additional responses or detailed explanations of other compensating controls as comments. You may add information regarding any planned releases or updates that would enhance the security of an application.

Also, use the space below to list any other security software controls that were not addressed in this questionnaire.

9. Comments

Additional: Please note in the comments section any other information that will be useful to the Hospital to review. For example:

- If the application will process or store credit card data and if so, has the credit processing module been certified as meeting PCI compliance?
- Will the application be included in the Hospital's domain, and if so, can the application be managed through Microsoft's Active Directory Group Policy Object (GPO)?

10. Company sign-off	
Instructions:	1. Complete and then print out the questionnaire. 2. Sign the questionnaire and print your name in the box below. 3. Scan the signed questionnaire and return by email to Privacy/Security officer at
Date completed:	**Signature: _____** **Printed Name: _____**
11. For Hospital Use Only – Information Security Review	
Date of review:	**Signature: _____** **Printed Name: _____**