IT Security Vendor Compliance Assessment

Description
This is a document of the general IT Security Compliance requirements that vendors must meet to have an application certified by the Columbia University Medical Center IT Security Department.

Overview
CUMC is committed to the compliance fitness of all CUMC systems in accordance with the following:

- Healthcare Insurance Portability and Accountability Act (HIPAA) of 2003
- Health Information Technology for Economic and Clinical Health (HITECH) of 2009

Compliance Design
CUMC has adapted HITRUST to insure certification of the security and compliance posture for HIPAA, HITECH, PCI/DSS, SSN and NIST guidelines.

CUMC uses the controls listed in this document to assess compliance. (See Compliance Requirements)

Testing and vulnerability scans will be done to ensure compliance of, but not limited to:

- Infrastructure (patches, configurations...)
- Web Applications (programming, configurations...)
- Network Architecture
- Host Configuration
System Facts
This section requires the Vendor to answer the following questions about the application and where it is located within CUMC.

1. Who is the department Administrator?

2. What will be the owning department name?

3. What is the Application name?

4. What will be the purpose of the application?

5. Who are the application custodians (day to day operations)?

6. Application classification (Web/Client-Server)?

7. If Web, will the IP address be required to be public or will a private address be acceptable?

8. What institution will own the hardware platform?

9. What institution will maintain the application?

10. Where will the hardware be located?

11. What institution will own the Application software?

12. Where will the data come from?

13. What will be the operating system used?

14. What database technology will be used?
15. Does the application handle electronic Protected Health Information (ePHI)?

16. Will the application handle Social Security Numbers?

17. Will the application handle driver’s license numbers?

18. Will the application handle credit card information?

19. Will the application publish to or be accessible from the Internet?

20. Will web access be secured by VPN/SSL?

21. If Internet access is not required, will it be shut down?

22. Will a Vendor have remote access and how is that access provided?

23. Will the application be accessible from mobile devices? Which ones? Is encryption enforced and how?

24. How many active users will there be? (per Day/per Month)

25. How many interfaces will there be?

26. Is Auditing and Monitoring available and if so how robust?

27. What is the upgrade, patch and maintenance plan and how is it implemented?

28. How robust is the authentication process?

29. Classify the application type as: (Clinical, Billing, Research, Educational, Business, FDA Regulated Research)
Compliance Requirements

This section requires the Vendor/Department to adhere to the following requirements for the application and where it will be located within CUMC. Any requirements that cannot be meet should be listed under issue’s with a suitable solution and submitted to the CUMC IT Security Office for approval

- **(01_b)** There must be a written procedure for granting and revoking user access that requires approval from a supervisor, with records of granted transactions and a process to remove terminated employees in a timely fashion.
- **(01_c)** Will there be supervisory approval required for administrative level access? Will there be a record of all privileges maintained?
- **(01_d)** Please make sure there are safe, up to date practices used including: strength, lockout, non-display, non-reuse, self-change, safe transmission and expiry.
- **(01_e)** All unattended computers are be protected with passwords, application timeouts (of 30 min. or less) and physical security (locks & cables).
- **(01_j)** There must be secure authentication required by policy on your system. Authentication should not be local; it should go through the central authority (exception for Research).
- **(01_l)** All access to network ports logically and physically are to be limited to approved administrators for all devices in the system architecture.
- **(02_d)** Work instructions, project plans and contracts must explicitly state tasks to implement and support security.
- **(02_e)** System custodians must be trained in security specific to your information assets.
- **(05_e)** All internal and confidential information must be protected through the use of a BAA process with consultants and vendors.
- **(06_c)** Is data retained for 7 years? Retained data must be protected according to its classification level. Example: (18 +7) for pediatric patients. See: http://www.health.state.ny.us/nysdoh/ems/policy/08-03.htm
- **(06_f)** All data created by the application owner/custodian must be encrypted on all portable media and devices and interfaces, including any computer that may contain data.
- **(08_a)** The system infrastructure must be physically secure.
- **(08_h)** Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.
- **(08_l)** All devices that contain data must be sanitized before they are disposed of.
- **(09_d)** Testing is prohibited on the production systems; there must be a test environment.
- **(09_h)** There must be capacity planning done to protect availability of the system.
- **(09_i)** There must be testing by the users and accepted before migration to production.
- **(10_h)** Security patches must be applied within at least 30 days? (Source Code Management)
- **(12_b)** you must have a risk assessment process for interruptions in your system availability.
☐ (12_c) There must be a BCDR plan that details the course of action to restore service or implement alternate services; it must be appropriately tested and reviewed on a least a yearly interval.

☐ There must be institutional security banners on authentication screens (including platform and subsystem authentications).

☐ (H7) Systems are to be scanned and corrected for vulnerability before placing in production environment. A few of the scans used my CUMC are listed below:
  - (IS1) NMAP
  - (IS2) NESSUS
  - (WS1) ACUNETIX

☐ (X1) The Robots.txt file on your site configured to inhibit Google or any search engine indexing.

Issues
Any issues that need to be resolved either before the requirement is implemented or before the implementation is complete need to be resolved or communicated to IT Security for approval. As the issues are resolved, those resolutions should be recorded as well. If the resolution of an issue changes the specification, update the documentation accordingly.