Security Assessment Template*

Step 1: Define the organization's current state

Step 2: Assess the degree to which the organization's systems currently comply – compare standards to current systems/practices and define gaps

Step 3: Determine intersections and impacts on current strategic plans – what is currently planned and how will that change in order to meet compliance standards?

Step 4: Prioritize gaps between current and future systems– from most critical to least critical

Step 5: Determine alternatives and solutions to close the gap

Step 6: Select the best solution (which may be to do nothing)

Step 7: Remediate/Implement/Acquire systems as needed

Areas of Organization Requiring Assessment

- Computers – hardware and location
- Application programs – system-wide and departmental
- Interfaces
- Communications infrastructure
  - Telephones
  - Fax machines
  - Connections and networks
  - Internet access
- Physical security around computers and networks
- Administrative safeguards including
  - Policies and procedures
    - Information Management Systems department
    - Departments
  - Security Awareness training
  - Contractual relationships and contracts
  - Back-ups and disaster recovery
- Personnel
  - Security Officer and Security Staff
  - Employee skill levels and workloads
  - Granting access to systems, password assignment
  - Authentication
  - Termination procedures

**Note: The Security Standards have not yet been finalized. This Template was designed to the proposed Security Standards.*

Security Assessment Template

Department Name _____

Section I: Department Profile	
Question:	**Explanation:**
1. How many employees are in your department? _____ Full-time employees _____ Part-time employees _____ Full-time equivalents _____ None	
2. Does your department contract with third parties for any data processing? (e.g., billing, data entry, transcription) ☐ Yes ☐ No	If yes, please list the names of the third parties/vendors, and briefly describe their responsibilities.
3. Are any of the individuals who work in your department not within the employ of the organization? ☐ Yes ☐ No	
4. Indicate the approximate number of employees by skill level: Licensed _____ Employees _____ External resources Trained and Certified _____ Employees _____External resources Professional / Administrative _____ Employees _____ External resources Other _____ Employees _____ External resources	

Department Name _____

Question:	Explanation:
5. Does your department **use** patient-related information? ☐ Yes (specify) ☐ No	If Yes, in what form? (Check all that apply.) ☐ Electronic ☐ Hard copy (paper, file, reports, etc.) ☐ Facsimile ☐ Oral
6. Does your department **access** patient-related information?	If Yes, in what form? (Check all that apply.) ☐ Electronic ☐ Via Email ☐ Hard copy (paper, file, reports, etc.) ☐ Facsimile ☐ Oral
7. Does your department **send or communicate** patient related information to anyone within the organization?	If Yes, in what form? (Check all that apply.) ☐ Electronic ☐ Via Email ☐ Hard copy (paper, file, reports, etc.) – internal recipient ☐ Hard copy (paper, file, reports, etc.) – external recipient ☐ Facsimile ☐ Oral
8. Are there formal policies and procedures that describe how patient-related information is to be sent or communicated within the organization? ☐ Yes ☐ No	Please list the policies and procedures and/or obtain copies of them.

Department Name _____

Question:	Explanation:
9. Does your department **send or communicate** patient related information to anyone outside of the organization?	If Yes, in what form? (Check all that apply.) ☐ Electronic ☐ Via Email ☐ Hard copy (paper, file, reports, etc.) – internal recipient ☐ Hard copy (paper, file, reports, etc.) – external recipient ☐ Facsimile ☐ Oral
10. Is the patient-related information that is sent or communicated to anyone outside of the organization sent across the Internet or any other open networks? ☐ Yes ☐ No	Please list the open networks your department uses: ☐ Internet ☐ Other: _____ ☐ Other: _____ ☐ Other: _____ ☐ Other: _____
11. Are there formal policies and procedures that describe how patient-related information is to be sent over open networks? ☐ Yes ☐ No	Please list the policies and procedures and/or obtain copies of them.
12. Is physical access to your departmental area limited to only those with a "need-to-know?" (Is your department locked or otherwise secured so that people who want to enter it must sign in or use a key or other means to enter?) ☐ Yes ☐ No	

Department Name _____

Question:	Explanation:
13. What kinds of people have access to or could access the areas of your department where individually identifiable health information is stored or accessed? (Check all that apply.) ☐ Department employees ☐ Employees from other departments (specify) ☐ Vendors (specify) ☐ Volunteers ☐ Students (specify) ☐ Physicians ☐ Patients and patient family members ☐ General public (unrestricted access) ☐ Other (specify) ☐ N/A	Please specify the types of individuals checked:
14. Do you have any responsibility to negotiate contracts? ☐ Yes (specify) ☐ No (specify)	If Yes, please describe process: If No, please provide name of individual or department responsible:

Department Name _____

Section II. Information Technology Usage

Question:	Explanation:
15. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (1) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)
16. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (2) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)
17. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (3) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)

Department Name _____

Question:	Explanation:
18. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (4) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)
19. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (5) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)
20. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (6) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)

Department Name _____

Question:	Explanation:
21. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, one of the Business Functions would be: Verifying insurance.)* • Business Function (7) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)
22. Identify a business function that your department routinely performs that requires patient-related information. *(For example, if your department is responsible for admitting patients, the Business Function would be: Admitting Patients.)* • Business Function (8) _____	What type of information technology, if any, is used to perform this Business Function? (**Check only one box.** If two boxes could be checked – for example, Departmental System and PC – either create another business function or check the box that represents how most of the function is performed.) ☐ Centralized Information System ☐ Departmental System ☐ Stand-alone PC ☐ Manual (no information technology used)
23. How many of the staff in the department have access to the Centralized Information System? ☐ Less than 5 ☐ 5 to 10 ☐ 11 to 20 ☐ More than 21 ☐ None	List the part(s) of the Centralized Information System that each staff member can access (by job title):

Department Name _____

Question:	Explanation:
24. How many of the staff in the department have access to a Departmental System? ☐ Less than 5 ☐ 5 to 10 ☐ 11 to 20 ☐ More than 21 ☐ None	List the Departmental System(s) that each staff member may access (by job title):
25. How many of the staff in the department have access to a Personal Computer? ☐ Less than 5 ☐ 5 to 10 ☐ 11 to 20 ☐ More than 21 ☐ None	List what program(s) are accessed by each staff member and on which PC(s) the programs reside (by job title):
26. Does each user in your department have his/her own individual user id and password? ☐ Yes ☐ No	
27. Does the individual user id and password differ by computer (Central Information System, Departmental System, PC, etc.) accessed? ☐ Yes ☐ No	

Department Name _____

Question:	Explanation:
28. Does the individual user id and password differ by application program accessed? ☐ Yes ☐ No	
29. Does the individual user id and password differ by function within the application program? ☐ Yes ☐ No	
30. Can individuals within your department access information or perform functions using the Central Information System or Departmental System that are not related to their normal job functions? ☐ Yes ☐ No	
31. Can an individual within your department be logged on to two or more different computers at the same time? ☐ Yes ☐ No	

Section III. Information Management – Administrative Procedures

Each covered entity must develop, formally document, implement, and maintain Administrative Procedures to guard Data Integrity, Confidentiality, and Availability. This section should be completed by management within the Information Management Systems department.

Question:	Explanation:
32. Are information technology systems and networks within the organization **Certified**? (**Certification** means the technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a specified set of security requirements.) ☐ Yes ☐ No	If yes, is such **Certification** performed internally or by an external accrediting agency? ☐ Internally ☐ By an external accrediting agency ☐ Both internally and by an external accrediting agency If by both, who is responsible for each system and network:
33. Is there a **Chain of Trust Agreement** with each of the organization's business partners with whom data is exchanged electronically? ☐ Yes ☐ No	
34. Does each **Chain of Trust Agreement** adequately protect the integrity and confidentiality of the data that is/will be electronically exchanged? ☐ Yes ☐ No	
35. Is there a written **Contingency Plan** that defines how the organization will respond to system emergencies? ☐ Yes ☐ No	

Question:	Explanation:
36. Does the **Contingency Plan** include procedures for: ☐ Performing backups? ☐ Yes ☐ No ☐ Preparing critical facilities that can be used if the primary facility cannot? ☐ Yes ☐ No ☐ Recovering from a disaster? ☐ Yes ☐ No	
37. Does the **Contingency Plan** include an applications and data criticality analysis? ☐ Yes ☐ No	
38. Does the **Contingency Plan** include a data backup plan? ☐ Yes ☐ No	
39. Does the **Contingency Plan** include a disaster recovery plan? ☐ Yes ☐ No	
40. Does the **Contingency Plan** include an emergency mode operation plan? ☐ Yes ☐ No	
41. Is there a **Formal Mechanism for Processing Records** (documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information)? ☐ Yes ☐ No	

Question:	Explanation:
42. Are there formal, documented policies and procedures for granting different levels of **Access** to health care information? ☐ Do the policies and procedures establish the rules for **Granting Access**? ☐ Yes ☐ No ☐ Do the policies and procedures provide for **Access Establishment** (determining the right of access)? ☐ Yes ☐ No ☐ Do the policies and procedures address **Access Modification**? ☐ Yes ☐ No	
43. Are **Internal Audits** routinely conducted to review the records of system activity such as logins, file accesses, security incidents? ☐ Yes ☐ No	
44. Are there documented practices to manage **Personnel Security**, particularly to assure appropriate supervision of personnel performing technical systems maintenance activities by authorized, knowledgeable people? ☐ Yes ☐ No	
45. Are there documented practices to manage **Personnel Security**, particularly to maintain a record of access authorizations (on-going documentation and review of the levels of access granted to a user, program, or procedure accessing health information)? ☐ Yes ☐ No	
46. Are there documented practices to manage **Personnel Security**, particularly to assure that operating and maintenance personnel have proper access authorization? ☐ Yes ☐ No	

Question:	Explanation:
47. Are there documented practices to manage **Personnel Security**, particularly personnel clearance procedures? ☐ Yes ☐ No	
48. Are there documented practices to manage **Personnel Security**, particularly establishing and maintaining personnel security procedures? ☐ Yes ☐ No	
49. Are there documented practices to manage **Personnel Security**, particularly to assure that system users, including maintenance personnel, receive security awareness training? ☐ Yes ☐ No	
50. Are measures, practices and procedures established and documented for the security of information systems? (**Security Configuration Management**) ☐ Yes ☐ No	
51. Do written security plans, rules, procedures, and instructions concerning all components of the organization's security exist? ☐ Yes ☐ No	
52. Is hardware and software installation and maintenance review and testing for security features documented? ☐ Connecting and loading new hardware and software? ☐ Yes ☐ No ☐ Periodic review of maintenance on hardware and software? ☐ Yes ☐ No ☐ Periodic security attributes testing on hardware and software? ☐ Yes ☐ No	

Question:	Explanation:
53. Does an inventory of the organization's hardware and software exist? ☐ Yes ☐ No	
54. Does the organization perform security testing including: ☐ Hands-on functional testing? ☐ Yes ☐ No ☐ Penetration testing? ☐ Yes ☐ No ☐ Verification testing? ☐ Yes ☐ No	
55. Does the organization routinely check for viruses and use virus-checking software? ☐ Yes ☐ No	
56. Have formal **Security Incident Procedures** been defined and documented to report security breaches? ☐ Report procedures? ☐ Yes ☐ No ☐ Response procedures? ☐ Yes ☐ No	

Question:	Explanation:
57. Is there a **Security Management Process** in place? ☐ Does the process include a Risk Analysis component? ☐ Yes ☐ No ☐ Does the process include a Risk Management component? ☐ Yes ☐ No ☐ Does the process address enforcement through Sanctions? ☐ Yes ☐ No ☐ Is there an overall security Policy that establishes needed levels of information security to achieve desired confidentiality goals? ☐ Yes ☐ No	
58. Is there a formal policy describing the appropriate security measures to implement upon termination of an employee or an internal/external user's access? ☐ Yes ☐ No	
59. Has the organization conducted Security Awareness Training for all personnel (including management)? ☐ Yes ☐ No	
60. Does the organization periodically disseminate Security Reminders? ☐ Yes ☐ No	
61. Are users educated on protecting their systems from viruses? ☐ Yes ☐ No	

Question:	Explanation:
62. Is the importance of monitoring login success or failure communicated to users? ☐ Yes ☐ No	
63. Do users receive training on how to report discrepancies? ☐ Yes ☐ No	
64. Does the organization conduct Password Management education sessions for users? ☐ Yes ☐ No	

Section IV. Physical Safeguards Protecting Computers and Systems

Each covered entity must develop, formally document, implement, and maintain Physical Safeguards to guard Data Integrity, Confidentiality, and Availability and to protect physical computer systems and related buildings and equipment from fire and other natural and environmental hazards and from intrusion. This section should be completed by management within the Information Management Systems department.

Question:	Explanation:
65. Has the organization identified one or more individuals responsible for security, specifically to manage and supervise the execution and use of security measures and personnel to protect data? ☐ Yes ☐ No	
66. Have **Media Controls** been established, and do these controls include and/or address: ☐ Access? ☐ Yes ☐ No ☐ Accountability? ☐ Yes ☐ No ☐ Data backup? ☐ Yes ☐ No ☐ Data storage? ☐ Yes ☐ No ☐ Disposal of electronic data and/or hardware containing such data? ☐ Yes ☐ No	

Question:	Explanation:
67. Has the organization documented and implemented **Physical Access Controls** including: ☐ Disaster recovery? ☐ Yes ☐ No ☐ A mode of operation that will enable the organization to continue operating in the event of a catastrophic event? ☐ Yes ☐ No ☐ Equipment controls (for bringing hardware in and out of the organization)? ☐ Yes ☐ No ☐ A facility security plan? ☐ Yes ☐ No ☐ Procedures for verifying access authorizations before granting physical access? ☐ Yes ☐ No ☐ Maintenance records? ☐ Yes ☐ No ☐ Need-to-know procedures for personnel access? ☐ Yes ☐ No ☐ Procedures to sign in visitors and provide escorts (if appropriate)? ☐ Yes ☐ No ☐ Testing and revision to formally authorized personnel? ☐ Yes ☐ No	

Question:	Explanation:
68. Has the organization established formal policies and guidelines on proper work station use (including what functions should be performed and the manner in which they are performed, e.g., logging off)? ☐ Yes ☐ No	
69. Are physical safeguards in place to minimize or eliminate the possibility that an unauthorized individual could access confidential health information through a work station? ☐ Yes ☐ No	
70. Does the organization conduct or sponsor Security Awareness Training for all employees, agents, and contractors to ensure their understanding of their security responsibilities? ☐ Yes ☐ No	

Section V. Technical Security Services – Information Protection and Individual Access

Each covered entity must develop, formally document, implement, and maintain Technical Security Services to guard Data Integrity, Confidentiality, and Availability. These processes are designed to protect information and to control individual access to information. This section should be completed for each hardware platform and for each application program.

Question:	Explanation:
71. Has the organization adopted formal access control policies and procedures ***for each computer and/or application program*** to address: ☐ Emergency access to information? ☐ Yes ☐ No ☐ One of the following types of access: ☐ Context-based access? ☐ Role-based access? ☐ User-based access? ☐ Does the access control mechanism used involve encryption? ☐ Yes ☐ No	
72. Are **Audit Controls** in place to record and examine system activity? ☐ Yes ☐ No	
73. Are **Authorization Controls** in place (mechanisms for obtaining consent for the use and disclosure of health information)? ☐ Yes ☐ No	
74. What type of access is employed in the **Authorization Controls**? ☐ Role-based access ☐ User-based access	

Question:	Explanation:
75. Does the organization have **Data Authentication** mechanisms in place to corroborate that data in its possession has not been altered or destroyed in an authorized manner? ☐ Yes ☐ No	
76. What type of **Data Authentication** mechanisms are employed? (Check all that apply.) ☐ Check sum ☐ Double keying ☐ Message authentication code ☐ Digital signature ☐ Other _____ ☐ Other _____	
77. Does the organization have **Entity Authentication** mechanisms in place to corroborate that an entity is the one it claims to be? ☐ Yes ☐ No	
78. Do the **Entity Authentication** mechanisms include: ☐ Automatic logoff so that an electronic session is terminated after a pre-determined time of inactivity? ☐ Yes ☐ No ☐ A unique user identifier that is assigned and maintained in security procedures to identify and track an individual's user identity? ☐ Yes ☐ No ☐ At least one of the following: ☐ Biometric identification? ☐ Password? ☐ Personal identification number?	

Question:	Explanation:
79. Do the **Entity Authentication** mechanisms include: ☐ A telephone call-back procedure to authenticate the identity of the receiver and sender of information through a series of questions and answers that are sent back and forth? ☐ Yes ☐ No ☐ A token? ☐ Yes ☐ No	

Section VI. Technical Security Mechanisms – Open Networks

Each covered entity must develop, formally document, implement, and maintain Technical Security Mechanisms to guard Data Integrity, Confidentiality, and Availability. These processes are designed to protect against unauthorized access to data that is transmitted over a communications network. This section should be completed for each communications system (network), and for each hardware platform or application program as appropriate.

Question:	Explanation:
80. Has the organization adopted formal **Communications or Network Controls**? ☐ Yes ☐ No	
81. Do the **Communications or Network Controls** include: ☐ Integrity controls to ensure the validity of the information being electronically transmitted or stored? ☐ Yes ☐ No **AND** ☐ Message authentication to ensure that a message received matches the message sent? ☐ Yes ☐ No	
82. Do the **Communications or Network Controls** also include: ☐ Access controls to protect communications transmitted over open or private networks so they cannot be easily intercepted and interpreted by parties other than the intended recipient? ☐ Yes ☐ No **OR** ☐ Encryption? ☐ Yes ☐ No	

Question:	Explanation:
83. Do the **Communications or Network Controls** include each of the following implementation features: ☐ An alarm device that can sense an abnormal condition within the system and provide a local or remote signal to indicate this abnormal condition? ☐ Yes ☐ No **AND** ☐ Audit trails to facilitate security audits? ☐ Yes ☐ No **AND** ☐ Entity authentication to irrefutably identify authorized users, programs, and processes and that denies access to unauthorized users, programs, and processes? ☐ Yes ☐ No **AND** ☐ Event reporting that will indicate operational irregularities in physical elements of a network or in response to the occurrence of a significant task? ☐ Yes ☐ No	