HIPAA Security Checklist for ___________________________ Health Department
Version 2 11/05/04

kam

R – Required
A – Addressable
M – MIS
L – Local Health Department
J – Joint (MIS / LHD)

			ADMINISTRATIVE SAFEGUARDS	Policies in place	Procedures in place	Date Completed
1			***Standard & Action* - Security Management Process: "Implement policies and procedures to prevent, detect, contain, and correct security violations."**			
2	**R**	J	***Action*** **- Risk Assessment:** "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity." □ Complete Risk Assessment Tool. □ Review Vulnerability Assessment report for your Health Department.	N/A	N/A	

3	**R**	J	***Action*** **- Risk Management:** "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306.(a): • Ensure confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains or transmits. • Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. • Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (Subpart E is HIPAA privacy). • Ensure compliance by its workforce." □ Take corrective action measures and document.	N/A	N/A	
4	**R**	M	***Action*** **- Sanction Policy:** "Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity." □ Ensure adequate policies are in place. Example: Progressive Discipline.	N/A	N/A	
5	**R**	J	***Action*** **- Information System Activity Review:** "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." □ OP – 18 – NTS Review □ IT 516 □ Work with OMIS, your service provider or create yourself procedures	N/A		

			for regular activity review.			
6	**R**	L	***Standard & Action*** **- Assigned Security Responsibility: "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."** □ Name of HIPAA Security Officer: _________________________________	N/A	N/A	
7		L	***Standard & Action*** **- Workforce Security: "Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to EPHI."** *Note: (a)(4) refers to Information Access Management below.* □ IP – (pending) □ OP – 08 (Darlene Review) □ OP – 15 (draft)			
8	A	L	***Action*** **- Authorization and/or Supervision:** "Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed."	N/A		

			□ Review your HIPAA privacy procedures and ensure they cover EPHI.			
9	A	L	***Action* - Workforce Clearance Procedure:** “Implement procedures to determine that the access of a workforce member to EPHI is appropriate.” □ OP – 15 (draft)	N/A		

10	A	L	***Action*** **- Termination Procedure:** "Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determinations made as specific in paragraph (a)(3)(ii)(B) of this section (Workforce Clearance Procedure above)." □ Use Network Delete form to terminate access to Network, shares, GroupWise etc... OP-08 (draft) □ OP – 08 (draft) □ OP – 19 (draft) □ Establish or document existing process for terminating access to applications such as Health Stat.	N/A		
11			***Standard & Action*** **- Information Access Management: "Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part."** (Subpart E is HIPAA privacy).	N/A	N/A	
12	A	J	***Action*** **- Access Authorization:** "Implement policies and procedures for granting access to a workstation, transaction, program, process or other mechanism." □ OP-15 (draft) □ IP pending			
13	A	J	***Action*** **- Access Establishment and Modification: "**Implement policies and procedures that, based upon the entity's access to authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process." □ OP-15 (draft)			

14		M	***Standard & Action*** **- Security awareness and training: "Implement a security and awareness training program for all members of its workforce (including management).** □ Implement state HIPAA security training program (not yet available)	N/A	N/A	
15	A	M	***Action*** **- Security Reminders:** "Periodic security updates". □ OP-22	N/A	N/A	
16	A	M	***Action*** **- Protection from Malicious Software:** "Procedures for protecting against, detecting and reporting malicious software: □ IT-0502 (7/2/04) □ OP-06 (4/27/04)	N/A		
17	A	J	***Action*** **- Log-In Monitoring:** "Procedures for monitoring log-in attempts and reporting discrepancies." □ Develop with your application vendor. □ OP – 25 (draft)	N/A		
18	A	J	***Action*** **- Password Management:** "Procedures for creating, changing and safeguarding passwords." □ OP- 14 (4/27/04)	N/A		
19		**J**	***Standard & Action*** **- Security Incident Procedures: "Implement policies and procedures to address security incidents."** □ OP – 18, 25 (draft) *"Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or the interference with system operations in an information system."*			

20	**R**	J	***Action* - Response and Reporting:** “Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.” □ OP-18 (draft)	N/A	N/A	
21		**L**	***Standard & Action* - Contingency Plan**: “Establish and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.” □ IP – 514 □ OP – 18, 23 (draft)			
22	**R**	J	***Action* - Data Backup Plan:** “Establish and implement procedures to create and maintain retrievable exact copies of EPHI.” □ OP-16 (3/8/04)	N/A		
23	**R**	L	***Action* - Disaster Recovery Plan:** “Establish (and implement as needed) procedures to restore any loss of data.” □ IT – 514 □ OP-07 (draft)			
24	**R**	L	***Action* - Emergency Mode Operations Plan:** “Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.” □ Establish procedures customized to your location. □ OP – 23 (draft)	N/A		

25	A	J	***Action* - Testing and Revision Procedures:** “Implement procedures for periodic testing and revision of contingency plans.” □ Establish procedures for periodic testing and revision. □ OP – 7, 23 (draft)	N/A		
26	**R**	J	***Standard* - Evaluation: “Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.”** □ Perform periodic evaluations. Document results.	N/A	N/A	
27		L	***Standard* - Business Associate Contracts and Other Arrangements. “A covered entity, in accordance with §164.306 (Security standards: General rules), may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.”** *(§164.314(a) is Business Associate Contracts or Other Arrangements.)*	N/A	N/A	

28	**R**	L	***Action*** - **Written Contract or Other Arrangement:** “Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).” *((b)(1) is Business Associate Contracts and Other Arrangements as listed directly above)* List EPHI Business Associates: ____________________ ____________________ ____________________ □ BAA’s on file with all EPHI business associates.	N/A	N/A	
			PHYSICAL SAFEGUARDS	Policies in place	Procedures in place	Date Completed
30		L	*Standard* - Facility Access Controls: “Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”			
31	A	J	***Action* - Contingency Operations:** “Establish (and implement as needed) procedures that allow facility access in support of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.” □ Establish procedures for local access. □ OP – 7, 23 (draft)	N/A		

32	A	L	***Action* - Facility Security Plan:** “Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.” □ Establish policies and procedures □ IT-513 in development			
33	A	L	***Action* - Access Control and Validation:** “Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.” □ Implement procedures. □ IT-513 in development	N/A		
34	A	**L**	***Action* - Maintenance Records:** Implement Policies and Procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). □ Implement policies and procedures □ IT-513 in development			
35	**R**	M	***Standard* - Workstation Use: “Implement Policies and Procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.”** □ Misc. IT policies and procedures. Specifics to be developed/revised. □ IT-513 in development			

36	**R**	L	***Standard* - Workstation Security: “Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users.”** □ Ensure physical safeguards are in place. □ IT-513 (under development)	N/A	N/A	
37			***Standard & Action* - Device and Media Control: “Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.”**			
38	**R**	M	***Action* - Disposal: “**Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.” □ OP-17 draft			
39	**R**	M	***Action* - Media Re-use:** “Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.” □ OP-17 draft	N/A		
40	A	L	***Action* –Accountability:** “Maintain a record of the movements of hardware and electronic media and any person responsible therefore.” □ Use “Shane’s tool” or develop your own.	N/A	N/A	
41	A	L	***Action* - Data Backup and Storage:** “Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.” □ Backup critical information before	N/A	N/A	

			moving equipment.			
			TECHNICAL SAFEGUARDS	Policies in place	Procedures in place	Date Completed
42		J	***Standard & Action*** **- Access Control: "Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to these persons or software programs that have been granted access rights as specified in §164.308(a)(4)."** *(§164.308(a)(4) is standard – Information Access Authorization as listed above.)*	N/A		
43	**R**	J	***Action*** **- Unique User Identification:** "Assign a unique name and/or number for identifying and tracking user identity." □ OP-08 draft □ Ensure unique user IDs are in place and that IDs are not shared.	N/A	N/A	
44	**R**	J	***Action*** **- Emergency Access Procedure:** "Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency." □ Establish procedures unique to your organization. □ OP-08 draft	N/A		
45	A	J	***Action*** **- Automatic Logoff:** "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity." □ Establish procedures with your application vendor if applicable.	N/A		
46	A	J	***Action*** **- Encryption and decryption:** "Implement a mechanism to encrypt and decrypt EPHI." □ Establish mechanism with your application vendor if applicable.	N/A	N/A	

47	**R**	J	***Standard*** **- Audit Controls: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI."** □ OP – 25 (draft) □ With your application vendor, ensure audit controls are in place. If not, enhance or replace your system.	N/A	N/A	
48			***Standard & Action*** **- Integrity: "Implement policies and procedures to protect EPHI from improper alteration or destruction."**			
49	A	J	***Action*** **- Mechanism to Authenticate EPHI:** "Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner"	N/A	N/A	
50	**R**	L	***Standard*** **- Person or Entity Authentication: " Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed."** □ OP – 26 (draft) □ Implement procedures.	N/A		
51			***Standard*** **- Transmission Security: "Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network."**	N/A	N/A	

52	A	M	***Action* - Integrity Controls:** “Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.” □ Identify all electronically transmitted EPHI.	N/A	N/A	

53	A	M	***Action* - Encryption:** "Implement a mechanism to encrypt EPHI whenever deemed appropriate." □ Identify all EPHI requiring encryption and implement mechanism.	N/A	N/A	
			ORGANIZATIONAL REQUIREMENTS			
54	**R**	L	**Business Associate Contracts:** See §164.314			
			POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
55			***Standard* - Policies and Procedures: "Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i),(ii),(iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart."**	N/A	N/A	

56		L	***Standard* - Documentation:** "(i) **Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and** **(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."** □ Ensure policies and procedures are in place for documentation and record keeping.			
57	**R**	L	***Action* - Time Limit:** "Retain the documentation required by (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. *((b)(1) is "Documentation" directly above)* □ link to all DHHR IT Policies, versions and effective dates: http://intranet.wvdhhr.org/Policies/IT/index.htm □ Ensure documentation is retained on all action requiring written record.	N/A	N/A	
58	**R**	L	***Action* - Availability:** "Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains." □ link to all DHHR IT Policies, versions and effective dates: http://intranet.wvdhhr.org/Policies/IT/index.htm □ Ensure retained documentation is available to appropriate persons.	N/A	N/A	
59	**R**	L	***Action* - Updates:** "Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI. □ Conduct periodic reviews.	N/A	N/A	