Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Business Associate Contracts and other Arrangements	BAA	31	Do you have policies prescribing required content of contracts and agreements that satisfy HITECH Act privacy and security requirements? 1. Content of contracts or agreements include: o Describe the permitted and required uses of protected health information by the business associate o Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law o Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract. Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). 2. Assurances to Safeguard information: o Authorization and monitoring of all connections from the information system to other information systems, i.e. a VPN connection from the provider's system to an EMR software vendor o The organization requires that providers of external information systems (i.e. EMR vendors) employ adequate			0	0	0	0	
Administrative Safeguards	Business Associate Contracts and other Arrangements	BAA	64	Does your organization have Business Associate agreements in place with third parties that have access to your patients information?			0	0	0	0	
Administrative Safeguards	Business Associate Contracts and other Arrangements	BAA	105	Does your organization work with third parties, such as IT service providers, that have access to your patients information?			0	0	0	0	
Administrative Safeguards	Business Associate Contracts and other Arrangements	BAA	115	Has your organization established written contracts or Business Associate Agreements with trading partners or Business Associates that documents satisfactory assurances the BA will appropriately safeguard information?			0	0	0	0	
Administrative Safeguards	Business Associate Contracts and other Arrangements	BAA	144	Review several new contracts (IS and other) to see the appropriate Business Associate Agreement is active and can be located.			0	0	0	0	
Administrative Safeguards	Compliance with Legal Requirements - Identification of applicable legislation	Legal Compliance	37	Does a process exist to identify new laws and regulations with IT security implications? (e.g., new state breach notification requirements)?			0	0	0	0	
Administrative Safeguards	Contingency Plan	AC Lists / IP	26	Do you enforce access to systems, equipment, and facilities through Access Control Lists (ACL's) for emergencies and disaster recovery?			0	0			
Administrative Safeguards	Contingency Plan	Alternative Resource Plans	6	Are there plans in place to handle/manage contingent events or circumstances (e.g. person with the key to the server is home sick)?			0	0			
Administrative Safeguards	Contingency Plan	Alternative Resource Plans	20	Do alternate work sites have appropriate administrative, physical, and technical safeguards? o Use of IPSec VPN for remote access to the network o Role-based access to data that allows access for users based on job function / role within the organization. o Use of Uninterruptable Power Supplies (UPS's) or generators in the event of a power outage to help ensure emergency access to computers, servers, wireless access points, etc. in the event of an emergency			0	0			

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Contingency Plan	Alternative Resource Plans	88	Does your organization have use of primary and alternate telecommunication services in the event that the primary telecommunication capabilities are unavailable? o The time to revert to the alternate service is defined by the organization and is based on the critical business functions o An example would be as simple as forwarding the main office number to an alternate office or even a cell phone			0	0	0	0	
Administrative Safeguards	Contingency Plan	Alternative Resource Plans	176	Has your organization identified an alternate processing facility in case of disaster?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Alternative Resource Plans	134	Is a copy of your recovery plan safely stored off-site?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Backup and Recovery	84	Does your organization have processes / procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure; this could include procedures to restore backup tapes to a new server in response to a hardware failure?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Backup and Recovery	175	Has your organization established and implemented procedures to create and maintain retrievable exact copies of ePHI? 1. Files identified as critical are documented and listed in the backup configuration 2. Exact copies of ePHI are created when needed before movement of equipment 3. Nightly backups of PHI performed which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility (it's recommended that the storage location be at least 60 miles away) 4. Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis), and restore test records kept 5. All backups encrypted using FIPS 140-2 compliant software and algorithms 6. Backups should be verified to help ensure the integrity of the files being backed up 7. Backup media are physically secured o Media (backup tapes, hard drives, removable media, etc.) should be stored in a locked safe while onsite, stored in a vault at an authorized facility when taken offsite o Media should be transported in an approved locked container 8. Multiple backups are retained as a failsafe 9. Backup media are made unreadable before disposal			0	0	0	0	
Administrative Safeguards	Contingency Plan	Backup and Recovery	112	Review several new contracts (IS and other) to see the appropriate Business Associate Agreement is active and can be located.			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	2	Are downtime procedures / plans tested for effectiveness? How often?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	5	Are staff aware of what needs to happen during computer downtime (planned or unplanned)?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	65	Does your organization have downtime procedures in place?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	74	Does your organization have policies and procedures for periodic testing and revision of contingency plans? o Training of personnel in their contingency roles and responsibilities; at least annually o Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results o Reviewing the contingency plan at least annually and revise the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing.			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	97	Does your organization review their contingency plan at least annually and revise the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	99	Does your organization test their contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	111	Has your organization established and implemented 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, restoration of lost data under the disaster recovery plan, and emergency mode operations plan in the event of an emergency (Contingency Plan); and is documentation of these policies and procedures up to date?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Contingency Policies and Procedures	113	Has your organization established and implemented procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Emergency Power	39	Does your data center have emergency power for orderly shut down of applications in the event of a power issue?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Physical Facility Access Security	174	Has your organization established and implemented policies and procedures to allow facility access in support of disaster recovery?			0	0	0	0	
Administrative Safeguards	Contingency Plan	Systems Access	38	Does our organization have 'Break-the-Glass' procedures in place to ensure there is a process in place so a person that normally would not have access privileges to certain information can gain access when necessary? o Any emergency accounts should be obvious and meaningful, i.e. breakglass1 o Strong password should be used o Account permissions should be set to minimum necessary o Auditing should be enabled			0	0	0	0	
Administrative Safeguards	Contingency Plan	Systems Access	73	Does your organization have policies and procedures for obtaining necessary PHI during an emergency as part of the Contingency Plan?			0	0	0	0	
Administrative Safeguards	Information Access Management	Agreements	95	Does your organization require all users sign non-disclosure / confidentiality / system usage agreement before authorizing access to systems, and annually? Confirm at least 25 people at each site have signed agreements up to date.			0	0	0	0	
Administrative Safeguards	Information Access Management	Agreements	102	Does your organization use nondisclosure agreements, acceptable use agreements, rules of behavior, Security awareness training and policy, and conflict-of-interest agreements?			0	0	0	0	
Administrative Safeguards	Information Access Management	Appropriate Access	114	Has your organization established Role-based access to data that allows access for users based on job function / role within the organization, and is it up to date? o This includes access to EMR systems, workstations, servers, networking equipment, etc.			0	0	0	0	
Administrative Safeguards	Information Access Management	Appropriate Access	77	Does your organization have policies and procedures that specify how and when access is granted to ePHI, EHR systems, laptops, etc. to only those individuals that require access?			0	0	0	0	
Administrative Safeguards	Information Access Management	Appropriate Access	82	Does your organization have procedures to determine if an employee's access to ePHI is appropriate?			0	0	0	0	
Administrative Safeguards	Information Access Management	Appropriate Access	87	Does your organization have processes and procedures for when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions. Appropriate actions include: o Returning old and issuing new keys, identification cards, and building passes o Closing of old accounts and establishing new accounts o Changing system access authorizations o Providing for access to official records created or controlled by the employee at the old work location and in the old accounts			0	0	0	0	
Administrative Safeguards	Information Access Management	Appropriate Access	118	Has your organization implemented policies and procedures for granting and maintaining appropriate access?			0	0	0	0	
Administrative Safeguards	Information Access Management	Audit	42	Does your organization audit systems for Last Login Inactivity and remove Ids if inactive over 90 days?			0	0	0	0	
Administrative Safeguards	Information Access Management	Audit	47	Does your organization conduct periodic audits of employees access to ePHI?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Information Access Management	Login Accounts	33	Do your accounts lock after 3 unsuccessful password attempts?			0	0	0	0	
Administrative Safeguards	Information Access Management	Login Accounts	34	Do your passwords include Microsoft logins (Active Directory Domain Controller or just locally logging into a computer) for each individual user?			0	0	0	0	
Administrative Safeguards	Information Access Management	Login Accounts	41	Does your organization allow shared access for any resource or system (i.e. computer or EHR system)?			0	0	0	0	
Administrative Safeguards	Information Access Management	Login Accounts	63	Does your organization have an approval process for activating and modifying accounts to laptops / workstations and EHR systems (i.e. network access request form requires appropriate signatures before creating or modifying a user account)?			0	0	0	0	
Administrative Safeguards	Information Access Management	Login Accounts	96	Does your organization require each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR system /software, or any other system or resource; and is each user assigned a unique identifier (i.e. user ID and password)?			0	0	0	0	
Administrative Safeguards	Information Access Management	Login Accounts	132	If your organization allows shared access for any resource or system (i.e. computer or EHR system), are these ids documented and limited?			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	191	Verify password strength of systems containing PHI, and 4 other systems (list systems verified).			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	35	Do your standard passwords meet the following criteria: o Password history is enforced so previous 4 passwords cannot be used o Minimum password length is set to 8 characters long o Passwords should contain 3 of the following criteria (complex passwords) a. Uppercase characters (A-Z) b. Lowercase characters (a-z) c. Numbers (0-9) d. Special characters (i.e. !,#,&,*) o Minimum password age is set so passwords can only be changed manually by the user after 1 day o Maximum password age is set so passwords should expire a. For systems that can accomodate complex passwords; every 180 days b. For systems that can not accomodate complex passwords; every 90 days			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	36	Do your systems display asterisks when a user types in a password?			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	40	Does your EHR system authenticate the user's identity before password change?			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	43	Does your organization change all default passwords that come with a product during product installation?			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	67	Does your organization have Password policies and procedures?			0	0	0	0	
Administrative Safeguards	Information Access Management	Passwords	70	Does your organization have policies and procedures for creating, changing, and safeguarding passwords?			0	0	0	0	
Administrative Safeguards	Information Access Management	Physical Access to PHI	101	Does your organization use cover sheets when transmitting patient communications via Fax, PHI is not left sitting on the fax machines, and are Fax numbers verified before transmission?			0	0	0	0	
Administrative Safeguards	Information Access Management	Physical Access to PHI	122	How are paper records secured to ensure confidentiality?			0	0	0	0	
Administrative Safeguards	Information Access Management	Systems Access	71	Does your organization have policies and procedures for denying access?			0	0	0	0	
Administrative Safeguards	Information Access Management	Systems Access	75	Does your organization have policies and procedures for providing access?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Information Access Management	Systems Access	86	Does your organization have processes and procedures for voluntary and involuntary terminations (full-time, part-time, temporary, contractors, etc.) including: o Process for disabling and removing accounts o Immediate disabling of any EMR user accounts o Immediate disabling of Windows accounts to workstations and/or servers o Termination of any other system access o Conduct exit interviews o Retrieval of all organizational property o Provides appropriate personnel with access to official records created by the terminated employee that are stored on the information system (i.e. computer, server, etc.)			0	0	0	0	
Administrative Safeguards	Information Access Management	Systems Access	98	Does your organization screen individuals (i.e. background checks) requiring access to organizational information and information systems before authorizing access?			0	0	0	0	
Administrative Safeguards	Information Access Management	VPN	9	Are your Vendor remote maintenance connections documented and fully secured?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Anti-virus	221	Does your organization have centralized administration, updating, and reporting of antivirus protection?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Anti-virus	72	Does your organization have policies and procedures for guarding against, detecting, and reporting malicious software?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Anti-virus	225	Does your organization have regularly scheduled antivirus scans of all systems, (i.e. weekly or monthly), and are all incoming files scanned real time?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Anti-virus	253	Is antivirus protection installed and operating effectively on every computer/server within the organization (i.e. McAfee, Symantec, etc.) in compliance with manufacturer recommendations, and latest patches are applied?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Anti-virus	254	Is antivirus protection updated at least daily; recommend every 4 hours?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Audit	12	Conduct audits on at least 15 Opt Out patients to make sure their data is kept confidential.			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Audit	11	Is a report run to determine unapproved, misused, and inappropiate software			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Encryption	230	Does your organization protect passwords (one way encryption or hashing) during storage?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Passwords	256	Is password protection turned on and in use for any devices or programs that allow it?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Awareness	30	Do you have notice on the login process at the first point of entry into the network stating: o the system is to be only used by authorized users o by continuing to use the system, the user represents he/she is an authorized user o where system capability permits, every user will be given information reflecting their last login date and time			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Awareness	32	Do you keep your computer user's work environment free of distractions when using technology? Assess work environments.			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Awareness	44	Does your organization clearly mark confidential communications as 'Confidential' when using interoffice envelopes?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Policies and Procedures	76	Does your organization have policies and procedures that facilitate the implementation of the security assessment, certification, and accreditation of systems?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	21	Do employees know what disclosures must be reported to HIS?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	22	Do employees know what to do in case of a privacy violation?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Security Awareness and Training	Security Training	1	Are all staff provided regular training on recognizing possible symptoms of viruses or malware on their computers?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	13	Describe how managers and other staff know when a BAA is required and how to facilitate obtaining a signed BAA?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	14	Do all staff know how to recognize symptoms of viruses or malware on their computers?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	24	Do Registration and clinical staff know what it means for patients to be placed on the Opt Out list?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	15	Do all staff understand and agree that they shall not hinder the operation of anti-virus software?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	16	Do all staff understand and agree to abide by access control policies?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	17	Do all staff understand and agree to abide by password policies?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	18	Do all staff understand and agree to abide by physical access policies and procedures?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	19	Do all staff understand the disaster recovery plan and their duties during recovery?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	23	Do employees know where to find HIPAA related policies?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	54	Does your organization have a procedure and/or training materials that address how staff are educated regarding: 1. When a patient authorization must be obtained prior to disclosing patient information 2. Who can sign an authorization to disclose patient information (e.g. minor, emancipated minor, deceased person, incapacitated person, etc.)			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	90	Does your organization provide a security awareness and training program for all members of its workforce, including management, that addresses the following: 1. Security awareness training to all users before authorizing access to the system, i.e. during new employee orientation. o HIPAA training o HIPAA training again prior to working in sensitive areas o Audits conducted yearly 2. The creation and maintenance of appropriate passwords, including the need to maintain password confidentiality. o Never share your user ID o Never share or reveal your password; at no time should an employee allow anyone else to access their accounts. o Initial password should be changed as soon as possible o Passwords are not written down or displayed on screen o Passwords are hard to guess, but easy to remember o All systems accessed with your ID are your responsibility 3. Education on nondisclosure agreements, acceptable use agreements, rules of behavior, Security policy, and conflict-of-interest agreements 4. Technology is available for business use o The organization has the right to monitor technology content and use o The organization has the right to disclose data; users should have no expectation of privacy 5. Employees are not authorized to retrieve or read any e-mail message not addressed to them, cannot use a password, access			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	91	Does your organization provide a security awareness and training program to educate users and managers for safeguarding of passwords?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	92	Does your organization provide security awareness training to all users before authorizing access to systems and on-going?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Security Training	121	How are management and staff made aware of who their security/privacy official is and how to contact her/him?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Security Awareness and Training	Security Training	124	How are staff made aware of process / procedure to report a confidentiality / security breach?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Systems Security	195	Are all workstations and servers regularly updated with the latest security patches, hotfixes, and service packs; updated every 30 days or when updates are released; are patches currently up to date?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Systems Security	10	Can your EHR system admin force password changes?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Systems Security	25	Do staff with responsibilities for maintenance understand and agree to system maintenance policies and procedures?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Systems Security	220	Does your organization have a system in place to monitor and block inappropriate website access?			0	0	0	0	
Administrative Safeguards	Security Awareness and Training	Systems Security	227	Does your organization have Spam protection that can be performed on the workstations themselves and/or at the gateway (entry/exit point into the network)?			0	0	0	0	
Administrative Safeguards	Security Management Process	Audit	46	Does your organization conduct continuous monitoring of information systems using manual and automated methods. a. Manual methods include the use of designated personnel or outsourced provider that manually reviews logs or reports on a regular basis, i.e. every morning. b. Automated methods include the use of email alerts generated from syslog servers, servers and networking equipment, and EMR software alerts to designated personnel.			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	222	Does your organization have peer to peer applications?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	28	Do you have a System security plan that specifies an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	45	Does your organization conduct a yearly assessment of security safeguards to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	48	Does your organization conduct Threat Analysis as new technologies and business operations are planned?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	50	Does your organization have a plan for periodic technical and non technical evaluation of standards in response to environmental or operational changes affecting the security of ePHI?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	108	Has your organization completed a Risk Management process to prevent, detect, contain, and correct security violations? Process should involve: 1. Initiation 2. Development or acquisition 3. Implementation 4. Operation or maintenance 5. Disposal			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	109	Has your organization completed a security Risk Analysis including identifying threats and vulnerability, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, results documentation, implementation of security updates, and correction of identified security deficiencies?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Security Management Process	Security Assessment	249	Has your organization's firewall been tested for appropriate configuration and security? 1. Policies are in place prescribing the use, configuration, and operation of firewalls and firewall logs 2. Access Control Lists 3. All computers are protected by a properly configured firewall 4. Guest devices are prohibited from accessing networks containing PHI 5. All staff understand and agree that they may not hinder the operation of firewalls. 6. VPNs - Do not access the server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Firewall should not have tcp port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software. 7. SSH Access instead of telnet 8. Updated firmware or Cisco IOS 9. Encrypted password 10. Firewall settings and activity logs periodically reviewed (at least annually) AND any time a new connection or configuration change is required 11. Firewall or border router prevents spoofing with outside incoming traffic by denying RFC 3330 (Special use address space) and RFC 1918 (Private internets) as the source address 12. ACL's (access control lists) are used on routers, switches, and firewalls to specifically allow or deny traffic (protocols, ports and services) though the devices and only on authorized			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	250	Has your organization's wireless been tested for appropriate configuration and security? 1. WPA/WPA2 encryption with strong passphrase o Use of WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit). o WPA/WPA2-Personal (the use of a pre-shared key) o Never use WEP because it is flawed, easy to crack, and widely publicized as such. 2. Strong password for admin login 3. MAC filtering 4. SSID Advertisement 5. Guest devices are prohibited from accessing networks containing PHI 6. Wireless intrusion protection			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	119	Have you categorized PHI identified within the organization and within the information system based on guidance from FIPS 199, which defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability); Potential impact options are Low, Moderate, or High?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	120	Have you identified PHI within the organization; ePHI you create, receive, maintain, transmit, and /or External sources of ePHI?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Assessment	138	Is the Implementation Methodology Security section filled out for all major systems?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Incidents	100	Does your organization track and document information system security incidents on an ongoing basis; is the database kept up to date?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	58	Does your organization have a process that addresses: the identification and measurement of potential risks, mitigating controls (measures taken to reduce risk), and the acceptance or transfer (Insurance policies, warranties for example) of the remaining (residual) risk after mitigation steps have been applied?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	29	Do you have documented information security policies and procedures, and formal processes in place for security policy maintenance and deviation?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	62	Does your organization have a senior person in the organization who signs and approves information systems for processing before operations or when there is a significant change to the system?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	66	Does your organization have formal sanctions against employees who fail to comply with security policies and procedures? Types of violations that require sanctions include the following: 1. Accessing information that you do not need to know to do your job. 2. Sharing computer access codes (user name & password). 3. Leaving computer unattended while you are logged into PHI program. 4. Disclosing confidential or patient information with unauthorized persons. 5. Copying information without authorization. 6. Changing information without authorization. 7. Discussing confidential information in a public area or in an area where the public could overhear the conversation. 8. Discussing confidential information with an unauthorized person. 9. Failing/refusing to cooperate with the compliance officer, ISO, or other designee 10. Failing/refusing to comply with a remediation resolution or recommendation Recommended disciplinary actions include: 1. Verbal or written reprimand 2. Retraining on privacy/security awareness, policies, HIPAA, HITECH, and civil and criminal prosecution 3. Letter of reprimand or suspension 4. Termination of employment or contract			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	81	Does your organization have policy in place for access of own records and those of minor children?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	85	Does your organization have processes /procedures to identify and respond to suspected or known security incidents? Processes / procedures should include: identifying incident, collecting and maintaining evidence, incident handling (report, contain, eradicate, recover), mitigate to the extent practicable, harmful effects of known security incidents, tracking and documentation of incidents and their outcomes, reporting incidents to the appropriate personnel, training of personnel for the handling and reporting of security incidents.			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	226	Does your organization have separate environments for system development, test, and production?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security Policies and Procedures	116	Has your organization implemented a Privacy Rule Administrative? Requirements include: 1. Appoint a HIPAA privacy officer 2. Training of workforce 3. Sanctions for non-compliance 4. Develop compliance policies 5. Develop anti-retaliation policies 6. Policies and Procedures			0	0	0	0	
Administrative Safeguards	Security Management Process	Security/Privacy Official	107	Has your organization assigned Security/Privacy Responsibility; identified the security/privacy official who is responsible for the development and implementation of required policies and procedures? If so, is the security/privacy official a full-time, dedicated position? o If "No", briefly describe other significant job responsibilities a. Provide an estimate of the percentage of time the official devotes to security/privacy related matters			0	0	0	0	
Administrative Safeguards	Security Management Process	Security/Privacy Official	126	How does the security/privacy official exercise oversight of privacy and security safeguard policies and procedures, including development, implementation, maintenance, and access by management/staff?			0	0	0	0	
Administrative Safeguards	Security Management Process	Security/Privacy Official	94	Does your organization report incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO)?			0	0	0	0	
Administrative Safeguards	Security Management Process	Separation of Duties	160	Are duties separated, where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of the organization's IT assets?			0	0	0	0	
Administrative Safeguards	Workforce Security	Physical Access to PHI	7	Are white/electronic boards, and patient lists are located out of public view and contain minimal patient information?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Administrative Safeguards	Workforce Security	Security Policies and Procedures	27	Do you have a security policy for third-party personnel, and do you monitor for compliance to the policy? o Third-party personnel include EMR vendors, outsourced IT functions, and any other thirdparty provider or contractor			0	0	0	0	
Administrative Safeguards	Workforce Security	Security Policies and Procedures	61	Does your organization have a Security policy for all personnel that is signed and updated regularly which specifies appropriate use on the systems, i.e. email communication, EMR access, keeping passwords safe, use of cable locks and privacy screens, etc.			0	0	0	0	
Administrative Safeguards	Workforce Security	Systems Security	3	Are only authorized personnel performing maintenance on information systems (including; EMR systems, workstations, servers, and networking equipment)?			0	0	0	0	
Administrative Safeguards	Workforce Security	Systems Security	8	Are your computers free of unnecessary software and data files?			0	0	0	0	
HIPAA Privacy Rule		"No Information" Patients	125	How are staff made aware that a patient is “no info”?			0	0	0	0	
HIPAA Privacy Rule		"No Information" Patients	127	How does your organization handle inquiries about “no information” patients?			0	0	0	0	
HIPAA Privacy Rule		"No Information" Patients	130	If a patient paid in full and asked that no information from his/her visit was shared with their insurance company, how should this request be handled?			0	0	0	0	
HIPAA Privacy Rule		"No Information" Patients	131	If there is one, what is the process that “automatically” classifies certain patients as “no information” patients (e.g., prisoners, VIPs, employees, etc.)?			0	0	0	0	
HIPAA Privacy Rule		Accounting of Disclosures Policies and Procedures	68	Does your organization have policies / procedures for accounting of disclosures? 1. Release of Information policies and procedures that includes the following: o Processes and procedures to track the disclosure of ePHI every time ePHI is disclosed (faxed, printed, electronically transmitted, etc) o Indication of why treatment, payment, or authorization information is being disclosed 2. Disclosures made through an EHR for payment/treatment/health care operation are included on the accounting 3. Process to allow an individual to obtain an accounting of disclosures made by Covered Entity & Business Associates or an accounting of disclosures by Covered Entity and a list of Business Associates with contact information o Business Associates must give individuals an accounting of PHI disclosures o The individual can get an accounting of payment/treatment/disclosure authorization/health care operation disclosures made during past 3 years 4. Appropriate procedures are in place for subpoenas, court orders, law enforcement, etc. for release of information. 5. Periodic audits are conducted			0	0	0	0	
HIPAA Privacy Rule		Accounting of Disclosures Policies and Procedures	151	Which restrictions may be denied, and which restrictions must be honored (including restrictions when the patient pays in full at time of service/treatment)?			0	0	0	0	
HIPAA Privacy Rule		Amendment Request Policies and Procedures	69	Does your organization have policies / procedures for when a patient requests an amendment (accepting an amendment, denying an amendment, actions on notice of an amendment, documentation)?			0	0	0	0	
HIPAA Privacy Rule		Minimum Necessary Data to Disclose Policies and Procedures	80	Does your organization have policies in place prescribing the 'minimum necessary' data to disclose for the following: 1. Uses 2. Routine disclosures 3. Non-routine disclosures 4. Ability to rely on request for minimum necessary			0	0	0	0	
HIPAA Privacy Rule		Minimum Necessary Data to Disclose Policies and Procedures	89	Does your organization limit disclosure or use of PHI to those that are authorized by the client, or that are required or allowed by the privacy regulations and state law, and to the minimum necessary to accomplish purpose?			0	0	0	0	
HIPAA Privacy Rule		Minimum Necessary Data to Disclose Policies and Procedures	143	Look at how each site is responding to law enforcement agency requests (police wanting blood draws, pictures, interview patients, etc).			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
HIPAA Privacy Rule		Minimum Necessary Data to Disclose Policies and Procedures	149	What kind of patient information is not included when a patient requests a copy of their records, and what is the process for excluding this information?(E.g., Psychotherapy notes; information compiled for use in civil, criminal, or administrative actions; information subject to prohibition by the Clinical Laboratory Improvements Act (CLIA); or Information that is not part of the designated record set.)			0	0	0	0	
HIPAA Privacy Rule		Minimum Necessary Data to Disclose Policies and Procedures	152	Who in your organization is responsible for reviewing disclosure requests to ensure only the minimum necessary amount of ePHI is disclosed?			0	0	0	0	0
HIPAA Privacy Rule		Notice of Privacy Practice	106	Does your organization's internet accurately reflect notice of privacy practice?			0	0	0	0	
HIPAA Privacy Rule		Notice of Privacy Practice	110	Has your organization developed and disseminated notice of privacy practice that includes at least the following: 1. The ways the Privacy Rule allows the covered entity to use and disclose protected health information. It must also explain that the entity will get patient permission, or authorization, before using health records for any other reason. o Review a copy of the standard authorization form used throughout the organization OR copies of varied authorization forms in use in the organization. Verify that the authorization form(s) contains any unique site-specific information, and the minimum following elements (take reasonable steps to limit the use or disclosure of, and requests for, [PHI] to the minimum necessary to accomplish the intended purpose): a. A description of the information to be used or disclosed b. The name of the person or organization authorized to make the disclosure c. The name of the person or organization to whom the information may be released d. An expiration date or event e. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, along with a description of how the individual may revoke the authorization f. A statement that the information used or disclosed under the authorization may be subject to redisclosure by the recipient and no longer protected under the Privacy Rule g. Signature of the individual and date			0	0	0	0	
HIPAA Privacy Rule		Notice of Privacy Practice	140	Is your organization's current version of the Notice of Privacy Practices distributed to all new patients?			0	0	0	0	
HIPAA Privacy Rule		Notice of Privacy Practice	141	Is your organization's current version of the Notice of Privacy Practices prominently displayed in all patient registration / waiting areas (e.g., inpatient registration, all outpatient registration areas, surgery waiting, any retail pharmacies)?			0	0	0	0	
HIPAA Privacy Rule		Patient Complaint	147	What is your organization's process for when a patient has a complaint related to their patient information?			0	0	0	0	
HIPAA Privacy Rule		Patient Information Review Policies and Procedures	4	Are patients/personal representatives supervised while they're reviewing records?			0	0	0	0	
HIPAA Privacy Rule		Patient Information Review Policies and Procedures	51	Does your organization have a policy/procedure that addresses cases in which a family member asks to review a patient's records during hospitalization or an office visit?			0	0	0	0	
HIPAA Privacy Rule		Patient Information Review Policies and Procedures	52	Does your organization have a policy/procedure that addresses cases in which a patient asks to review his records during hospitalization or during an office visit?			0	0	0	0	
HIPAA Privacy Rule		Patient Information Review Policies and Procedures	53	Does your organization have a policy/procedure that addresses how patients can gain access to their protected health information?			0	0	0	0	
HIPAA Privacy Rule		Patient Information Review Policies and Procedures	60	Does your organization have a process to review requests for patient information for research purposes?			0	0	0	0	
HITECH Act		Accounting of Disclosures Policies and Procedures	56	Does your organization have a process for Handling Requests to Restrict Disclosure? The covered entity must comply with the requested restriction if: - Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment) - The protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
HITECH Act		Alternative Means of Communication Request Policies	79	Does your organization have policies for alternative means of communication requests?			0	0	0	0	
HITECH Act		Breach	55	Does your organization have a process for determining if an incident meets the HHS OCR definition of a "breach", particularly how you determine the potential for risk of harm to the patient?			0	0	0	0	
HITECH Act		Breach	57	Does your organization have a process for notification to the following in the event of a breach of unsecured PHI: - Individuals - Media - Secretary of HHS			0	0	0	0	
HITECH Act		Disclosure PIN #s	103	Does your organization use PIN #s for disclosure of patient information?			0	0	0	0	
HITECH Act		Minimum Necessary Data to Disclose Policies and Procedures	142	Look at authorizations within HIS as it relates to subpoenas, court orders, etc to make sure PHI is protected as outlined in the facility policy, and the information submitted was the minimum amount required.			0	0	0	0	
HITECH Act		Patient Information Review Policies and Procedures	59	Does your organization have a process to determine if a patient authorization is needed prior to disclosing patient information for research purposes?			0	0	0	0	
HITECH Act		Patient Information Review Policies and Procedures	145	What fees does your organization charge patients for copies of records (e.g., costs for copying, retrieval fee, fee to review, fee for multiple copies, etc.)?			0	0	0	0	
HITECH Act		Patient Information Review Policies and Procedures	146	What is the process by which physicians are made aware of the requirement for patient authorization before viewing records of family members and/or friends?			0	0	0	0	
HITECH Act		Patient Information Review Policies and Procedures	148	What is your organization's process when patients or personal respresentatives come in to review records or pick up copies of records?			0	0	0	0	
HITECH Act		Use of Patient Information Documentation	49	Does your organization document decisions as they relate to use of patient information (and whether patient authorization is needed) for research?			0	0	0	0	
IS Management		Security Awareness	258	Are Security Sanction meetings being attended, and minutes published?			0	0	0	0	
IS Management			135	Is an appropriate IS leadership committee structure in place at all hospitals?			0	0	0	0	
IS Management			137	Is Succession Planning in place (appropriate succession plans are in place for IS management with education / mentoring to potential internal candidates)?			0	0	0	0	
IS Management			139	Is there an IS Strategic Plan in place?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Anti-virus	205	Do handheld or mobile devices that support anti-virus software have it installed and operating effectively?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Access to PHI	157	Are all hospitals following policies and procedures for the disposal of equipment and media?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Access to PHI	166	Does your organization have processes and procedures for removal of ePHI from electronic media before the media are available for reuse?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Access to PHI	169	Does your organization perform degaussing of media?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Access to PHI	170	Does your organization perform DoD approved wiping of media before reuse, and before destroying media? o DoD wiping involves writing over the hard drive with random data 7 times before it's considered unrecoverable			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Access to PHI	177	Has your organization implemented 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?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Access to PHI	178	Has your organization implemented policies and procedures to address final disposition of ePHI, and/or hardware or electronic media on which it is stored (media, hard drives, copiers, fax machines, etc)?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Security	158	Are computers protected from environmental hazards? o Positioning of equipment to help minimize potential damage from fire, flood, and electrical interference.			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Security	183	Is equipment located in high-traffic or less secure areas physically secured?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Physical Safeguards	Device and Media Controls	Physical Equipment Security	184	Is media (backup tapes, hard drives, removable media, etc.) stored in a locked safe while onsite, stored in an approved locked container when transported, and stored in a vault at an authorized facility when taken offsite?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Security	185	Is media transported by authorized personnel, secured in a locked container, and encrypted using FIPS 140-2 compliant software or algorithms?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Security	168	Does your organization maintain a list of mobile devices that have been tested and approved for use?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Tracking	252	Is a list of Modems in use kept and maintained? Verify / check usage.			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Tracking	156	Are all devices containing PHI inventoried, and can they be accounted for?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Tracking	167	Does your organization keep records that show who has what equipment?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Tracking	171	Does your organization record movements of hardware and electronic media and the person responsible for its movement?			0	0	0	0	
Physical Safeguards	Device and Media Controls	Physical Equipment Tracking	182	Is Capital equipment asset tagged?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Audit	172	Does your organization regularly monitor Key distribution and Badge access is issued to appropriate staff? Verify Key distribution and Badge access is issued to appropriate staff.			0	0	0	0	
Physical Safeguards	Facility Access Controls	Audit	189	Review public area countertops and ensure they're free from paper PHI records; lobby, check-in desks, etc, and patient records are not left unattended.			0	0	0	0	
Physical Safeguards	Facility Access Controls	Audit	188	Review data center security (onsite computer room); check proximity badge log, unauthorized access attempts, etc.			0	0	0	0	
Physical Safeguards	Facility Access Controls	Facility Policies and Procedures	78	Does your organization have policies and procedures that specify physical and environmental safeguards used?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Facility Policies and Procedures	179	Has your organization implemented 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)? 1. Policies and procedures that specify maintenance to the facility 2. Change management process that allows request, review, and approval of changes to the information system or facility 3. Spare parts available for quick maintenance of hardware, doors, locks, etc.			0	0	0	0	
Physical Safeguards	Facility Access Controls	Facility Policies and Procedures	153	Who is responsible for ensuring only appropriate persons have keys or codes to the facility and locations within the facility with ePHI?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Access to PHI	164	Does your organization ensure appropriate confidential space exists so conversations regarding PHI and patient examinations/interviews regarding PHI are conducted quietly in private areas (not in elevators, bathrooms, cafeteria, etc)?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Access to PHI	181	If your organization does not use shredders for disposal of documents of a confidential nature or contain PHI, are documents put in recycle bins, not kept in the open, bins empied on a regular basis, and are kept locked if in public areas.			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Access to PHI	104	Does your organization use shredders for disposal of all documents of a confidential nature or contain PHI?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Facility Access Security	154	Are changes made to locks, keys, combinations when lost, stolen, or staff terminated?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Facility Access Security	155	Are cipher locks and/or card access control systems in use to access sensitive areas of the facility?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Facility Access Security	161	Are physical access to secure areas limited to authorized individuals?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Physical Safeguards	Facility Access Controls	Physical Facility Access Security	180	Has your organization implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control? 1. Enforcement through Access Control Lists (ACL's) 2. Policy and procedures that specify physical and environmental safeguards used. 3. A list of personnel with authorized access to specific areas. If a card-access system is used then the list can be generated by the card-access system. 4. The use of cipher locks and/or card access control system to sensitive areas of the facility 5. Monitoring physical access through the use of cardaccess system, i.e. Keri access control system 6. Monitoring physical access through the use of video cameras 7. Controls physical access by authenticating visitors at the front desk (or other sensitive areas) before authorizing access to the facility o Presenting an authorized badge or ID for access o Records of physical access are kept that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. o Designated personnel within the facility review the visitor access records daily.			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Facility Access Security	186	Is physical access to wiring closets monitored (access logs, alarms, cameras, escorts)?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Facility Security	165	Does your organization have a fire suppression and detection device/system?			0	0	0	0	
Physical Safeguards	Facility Access Controls	Physical Facility Security	187	Is temperature and humidity in wiring closets monitored and maintained?			0	0	0	0	
Technical Safeguards	Access Controls	AC Lists / IP	239	Does your organization use IP Address and Access Control Lists to allow or deny access to the EHR system or other resource?			0	0	0	0	
Technical Safeguards	Access Controls	AD Policies	251	Have you disabled the ability for users to write data to USB & CD/DVD Drives through the use of Group Policies or enforced locally on the workstations? o Writing should only be allowed if FIPS 140-2 compliant encryption is utilized			0	0	0	0	
Technical Safeguards	Access Controls	Appropriate Access	196	Are computers and mobile devices that contain, or have connections to ePHI, configured to prevent unauthorized use?			0	0	0	0	
Technical Safeguards	Access Controls	Appropriate Access	218	Does your organization ensure common electronic media (share folders, drives, etc) contain no PHI or confidential data?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	93	Does your organization regularly conduct audits and site inspections?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	123	How are physical access controls authorized and monitored?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	128	How long does your organization maintain audit records?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	129	How routinely does your organization review audit records?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	194	Where and how does your organization store audit records?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	190	Verify computers logged off or locked when not attended (on-going, at all hours).			0	0	0	0	
Technical Safeguards	Access Controls	Audit	192	Verify passwords are not posted on computers or in public areas.			0	0	0	0	
Technical Safeguards	Access Controls	Audit	193	Verify Windows screen-saver locks workstation after 5 minutes of inactivity (on-going, at all hours).			0	0	0	0	
Technical Safeguards	Access Controls	Audit	199	Are EMR and other audit logs enabled, monitored and reviewed regularly, and email alerts setup for login failures, elevated access, and other events?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	213	Does your EHR software log and track all access which specifies each user?			0	0	0	0	
Technical Safeguards	Access Controls	Audit	248	Has your organization enabled, and do you monitor, Windows Security Event Logs (workstation and servers), and other application and system event Logs?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Technical Safeguards	Access Controls	Audit	117	Has your organization implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, and routine security monitoring and reporting in information systems? 1. Policy and procedures that specify audit and accountability 2. Procedures for monitoring login attempts and reporting discrepancies 3. Examples of auditable events include, but not limited to: o Account creation o Account modification o Account disabled o Account escalation o Server health o Network health o Access allowed o Access denied o Service installation o Service deletion o Configuration changes o Password strength o Log out o Security patches 4. Ensure audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component); (iii) type of event; (iv) user/subject identity; and (v)			0	0	0	0	
Technical Safeguards	Access Controls	EMR PDA Security	224	Does your organization have Personal Data Assistant (PDA) security in place (encryption, 10 login attempts and PDA cleared, etc)?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	215	Does your organization encrypt / secure data at rest (PHI and other confidential), including laptops, thumb drives and other media?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	216	Does your organization encrypt all electronic transmission of PHI (ePHI)?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	217	Does your organization encrypt removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.)? o All media used in fulfilling requests for electronic copies of PHI			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	238	Does your organization use full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.)? Any solution should be FIPS 140-2 compliant as specified in NIST 800-111.			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	255	Is ePHI encrypted when on computers and mobile devices?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	198	Are connections from computers and mobile devices to EHRs encrypted?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	207	Do you use a central management system for the encryption of removable media including USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.)?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	219	Does your organization ensure passwords can only be accessed and interpreted by the authentication mechanism?			0	0	0	0	
Technical Safeguards	Access Controls	Encryption	246	Does your organization use wireless encryption?			0	0	0	0	
Technical Safeguards	Access Controls	Passwords	200	Are passwords enforced in your EMR system, Active Directory, or at least on the local workstation or server?			0	0	0	0	
Technical Safeguards	Access Controls	Physical Access to PHI	197	Are computers running EHR systems shielded from unauthorized viewing? o The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of ePHI. o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc. o Windows screen-saver should lock your workstation after 5 minutes of inactivity			0	0	0	0	
Technical Safeguards	Access Controls	Physical Access to PHI	162	Are printers and Fax machines located where sensitive data cannot be accessed by unauthorized personnel?			0	0	0	0	
Technical Safeguards	Access Controls	Physical Access to PHI	159	Are computers running healthcare-related systems unavailable for other purposes?			0	0	0	0	
Technical Safeguards	Access Controls	Remote File Sharing and Printing	257	Is remote file sharing and printing (including remote printing) disabled?			0	0	0	0	
Technical Safeguards	Access Controls	Security/Privacy Official	150	What system does the security/privacy official have in place to routinely monitor and audit potential risk areas?			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Technical Safeguards	Access Controls	SSL/TLS	`	Does your organization use SSL/TLS for web-based access to EHR software? o Use of a centralized certificate server to assign certificates to Active Directory users and computers			0	0	0	0	
Technical Safeguards	Access Controls	System Session	228	Does your organization limit concurrent user Active Directory sessions to 3?			0	0	0	0	
Technical Safeguards	Access Controls	System Session	163	Do you enforce session lock after 10 minutes (no more than 30 minutes) of inactivity on the computer system? o This can be enforced through Active Directory Group Policies if in a Windows Domain environment or at least set locally on the computer if not on a domain			0	0	0	0	
Technical Safeguards	Access Controls	System Session	208	Does your remote access (VPN access) and portable devices (laptops, PDA's, etc.) sessions lock within 30 minutes of inactivity?			0	0	0	0	0
Technical Safeguards	Access Controls	System Session	210	Do your users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter)?			0	0	0	0	0
Technical Safeguards	Access Controls	System Session	247	Does your Windows screen-saver lock your workstation after 5 minutes of inactivity?			0	0	0	0	0
Technical Safeguards	Access Controls	System Session	209	Do your terminal services or Citrix sessions terminate after 30 minutes of inactivity?			0	0	0	0	
Technical Safeguards	Access Controls	System Session	211	Do your VPN sessions terminate after 30 minutes of inactivity?			0	0	0	0	
Technical Safeguards	Access Controls	System Session	212	Does your EHR session terminate after 20 minutes of inactivity?			0	0	0	0	
Technical Safeguards	Access Controls	Systems Access	203	Can every user account be positively tied to a currently authorized individual?			0	0	0	0	
Technical Safeguards	Access Controls	Systems Access	204	Can every user identity be identified and tracked?			0	0	0	0	
Technical Safeguards	Access Controls	Systems Access	223	Does your organization have Person or Entity Authentication procedures to verify that the person or entity seeking access ePHI is the one claimed?			0	0	0	0	
Technical Safeguards	Access Controls	Systems Security	201	Are systems and applications updated or patched regularly as recommended by the manufacturer?			0	0	0	0	
Technical Safeguards	Access Controls	Systems Security	206	Do you control and monitor all remote access through the use of a syslog server, VPN server, and Windows Active Directory and/or Cisco Access Control Server (ACS)?			0	0	0	0	
Technical Safeguards	Access Controls	Tokens, Biometrics, and/or Certificates	133	If your organization uses authenticators (i.e. security tokens, PKI certificates, biometrics, passwords, and key cards), how do you manage the authenticators? Management includes procedures for initial distribution, lost/compromised or damaged authenticators, or revoking of authenticators.			0	0	0	0	
Technical Safeguards	Access Controls	Tokens, Biometrics, and/or Certificates	245	Does your organization use tokens, biometrics, and/or certificates in addition to standard passwords?			0	0	0	0	
Technical Safeguards	Access Controls	VPN	240	Does your organization use IPSec VPN for remote access to the network?			0	0	0	0	
Technical Safeguards	Access Controls	VPN	242	Does your organization use passwords and/or tokens for remote access through a Virtual Private Network (VPN)?			0	0	0	0	
Technical Safeguards	Access Controls	Windows Domain Controller	241	Does your organization use Microsoft Active Directory (Windows Domain Controller) to permit only authorized computers on the domain?			0	0	0	0	
Technical Safeguards	Integrity	Encryption	233	Does your organization use cryptographic hashing functions such as SHA?			0	0	0	0	
Technical Safeguards	Integrity	Encryption	237	Does your organization use file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP)?			0	0	0	0	
Technical Safeguards	Integrity	Encryption	243	Does your organization use PKI for email communication to help ensure both confidentiality and integrity of the message?			0	0	0	0	
Technical Safeguards	Integrity	Security Incidents	232	Does your organization use audit reduction, review, and reporting tools (i.e. a central syslog server) to support after-the-fact investigations of security incidents without altering the original audit records?			0	0	0	0	
Technical Safeguards	Integrity	Systems Security	236	Does your organization use Endpoint security solutions (i.e. McAfee Enterprise, Cisco CSA, Symantec Endpoint, etc) to prevent unauthorized modification to software running on computers or servers?			0	0	0	0	
Technical Safeguards	Integrity	Systems Security	136	Is Change Control used by all IS areas? Have managers provide evidence.			0	0	0	0	
Technical Safeguards	N/A	Audit	214	Does your organization conduct regular site Licensing audits (at least 1 application per quarter)? Verify we have completed continuing audits on our major applications.			0	0	0	0	

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
Technical Safeguards	Transmission Security	Audit	231	Does your organization use a central syslog server for monitoring and alerting of audit logs and abnormalities on the network including: o Account locked due to failed attempts o Failed attempts by unauthorized users o Escalation of rights o Installation of new services o Event log stopped o Virus activity			0	0	0	0	
Technical Safeguards	Transmission Security	Audit	229	Does your organization monitor logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls?			0	0	0	0	
Technical Safeguards	Transmission Security	Encryption	235	Does your organization use email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server), and do you test the system at least annually? o PKI for email communications			0	0	0	0	
Technical Safeguards	Transmission Security	Physical Facility Security	202	Are transmission lines protected and secured (wiring closet locked, cables in conduit)?			0	0	0	0	
Technical Safeguards	Transmission Security	Tokens, Biometrics, and/or Certificates	234	Does your organization use digital certificates for email communications?			0	0	0	0	

Status Rating Key:
Immediate work
Minor work needs completing
Compliant

Date:

Prepared By:

Contributors:

Approved by:

Security Management Process : Implement policies and procedures to prevent, detect, contain, and correct security violations.	Assigned Security Responsibility										
164.308 (a)(1)	Workforce [illegible]										
164.308 (a)(2)	[illegible]										
164.308(a)(3)	Awareness and										
164.308(a)(4)	Security Incident [illegible]										
164.308(a)(5)	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 electronic PHI.										
164.308(a)(6)	Evaluation										
164.308(a)(7)	Business [illegible]										

Safeguard	Standard	Category		Question	Policy/Supporting Documentation	2013 Munson - Answer	2014 Munson-Answer	Follow Up (if needed)	Status Rating	Risk Rating	
164.308(a)(8)	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.										
164.308(b)											
164.310(a)											