SAMPLE TEMPLATE
SRA –

Protect Electronic Health Information
Security Risk Analysis

INSERT DATE OF ANNUAL SRA

The INSERT YEAR Security Risk Analysis to re-assess the protection of electronic patient health information was conducted for INSERT GROUP NAME. The practice has an ongoing security risk assessment in place, being focused on continuous quality improvement. During the early spring, summer and fall of INSERT YEAR, internal efforts focused to review, identify and make updates to policies as well as to complete a full review of the practice overall operations were undertaken.

As part of the assessment process, the Corporate Compliance Officer and the Privacy and Security Official, met together several times and reviewed in detail from the US Department of Health and Human Services (HHS) and the Office of the National Coordinator for Health Information Technology (ONC) the Security Risk Assessment Tool, specifically the physical, technical and administrative safeguards components. The Privacy and Security Official also completed for the practice the online Security Risk Assessment Tool. Action has been taken to address policies in need of updating. In addition, the practice's overall Compliance Program, business associate agreements, and employee confidentiality statements were also reviewed and updated. Planning is underway now to prepare for improvements for the 2019 Compliance Training.

Physicians and NPI's: INSET ALL BELOW

Tax ID: INSERT

Group NPI # - INSERT

Medicare # (PTAN) - INSERT

Security Management Process: 164.308(a)(1)

1. Security Analysis of Network – The practice utilizes a real-time INSERT DETAILS ON ANTI VIRUS AND FIREWALL and also has ongoing measures in place as documented in our policies that address this.

2. Security Analysis of Computer system – an evaluation has been completed of the computer system to verify that appropriate security measures are in place

Implementation Specifications:

1. Risk Analysis – this has been completed as noted above and is an ongoing process.
2. Implementation of Security Measures – the practice has identified and selected security features to implement. Current policies are in place to ensure appropriate administrative, technical and physical safeguards are in place.
3. Sanction Policy- there have been no cases of workforce members who fail to comply with security policies and procedures
4. Information System Activity Review - 164.308(a)(1)(ii) (A-D)
    a. Audit logs- monthly audits are completed and are on file
    b. Access reports monthly audits are completed and are on file
    c. Security incident tracking – a process is in place to track security incidents and follow up with corrective action
    d. Written security policy – detailed policy manual is in place and updated on annual basis or more frequently as needed
    e. Testing of appropriate security features in place and adequate to meet needs- testing is in place
    f. Safeguards in place for data integrity, confidentiality, availability by access control, audit control, authorization control and data authentication- safeguards are in place and policies exist for all that are updated at least on an annual basis
    g. Regular and ongoing audit of practice's computer system records- these are completed on regular basis by Privacy and Security Official
5. Assigned Security - 164.308(a)(2)
    a. Corporate Compliance Officer – job description – INSERT NAME
    b. Privacy Security Official – job description – INSERT NAME
    c. Physician Compliance/Security Officer- INSERT NAME MD
6. Workforce Security - 164.308(a)(3)(i) and (ii)
    a. Security training for all employees- performed on annual basis with updated information
    b. Designated staff members and vendor to handle hardware and software challenges, access to and maintenance of servers, software training and technical challenges- completed by Privacy and Security Official
    c. Assignment of Supervisory Access to Security Official- this is the Privacy and Security Official
    d. Temporary passwords are assigned to non-permanent employees to access the system as needed and are disabled upon completion of work assigned.

e. Temporary employees complete HIPAA privacy and security training and are provided temporary passwords – yes this is completed
f. Different levels of security are assigned to different staff members depending on job responsibilities- yes different levels are set up
g. Outside Transcription Service- The practice continues to have INSERT AS APPLICABLE an outside on demand transcription service available with a current contract and business associate agreement. This is available as a backup system.
h. Formal, documented instructions are in place to ensure that terminated employees or other users, including temporary employees, no longer have access to confidential data. The practice has procedures in place to terminate both the Windows log on and EMR log on, as well as access to the INSERT DETAILS hospital portals, Tiger Text and work email. All building access via assigned key fobs are collected prior to termination and departure.

7. Information Access Management - 164.308(a)(4)(i)
    a. The practice utilizes passwords to verify authorized users.
    b. The practice restricts physical access controls to authorized personnel only.
    c. Designated staff is set up and in place for Security Official/IT Manager to load software applications and needed upgrades to practice PC equipment.
    d. Network file sharing is set up by Security Official
    e. Temporary passwords are given out on a time limited basis to non-employees in order to conduct necessary business. This access is terminated quickly once the task has been completed and is monitored throughout.
    f. Dial up/Remote Access is set up following established policies and procedures
    g. The practice has procedures in place to ensure only authorized individuals have physical access to information and unauthorized users do not
    h. The practice has a process in place to modify an entity's level of access to ePHI
8. Security Awareness and Training - 164.308(a)(5)(i)
    a. Periodic security updates and information reminders are provided monthly to all staff
    b. Annual security training is provided to all employees
    c. Use of virus and firewall software policies and procedures are in place and monitored on monthly basis
    d. Security measures are in place to handle information downloads
    e. Other methods of data downloads including CD Roms and USB drives are utilized and closely monitored.

f. The practice accesses the Internet through its network
g. An Internet Firewall is in place at the practice
h. There is tracking in place to monitor accessing of software at the practice
i. There is tracking in place to monitor dial up and remote access – INSERT DETAILS AS APPLICABLE
j. The practice maintains a record of EMR monthly log of network access by staff and physicians. Logs are also created for the shared file folders and domain controller.
k. Monthly log of EMR user access logs is maintained
l. Passwords are set up for individual access to EMR system, as well as the hospital portals. A monthly report is completed for EMR and Windows password lock outs.
m. Emergency procedure for accessing EPHI – Break the Glass Policy-
n. Temporary and permanent employees do NOT share passwords.
o. The practice does allow for password protection of documents as needed.
p. In the event of lost laptops or iphones, the practice has a policy and system in place to disable passwords to ensure security is maintained. All practice laptops utilize full disk encryption when needed and no unencrypted ePHI is stored on the laptops or iPhones.
q. Networks access is governed by passwords.
r. Passwords are changed on a regular basis.
s. User access logs are reviewed on a monthly basis.

9. Security Incident Procedure - 164.308(a)(6)(i)
    a. Security incident policy is in place
    b. Procedures are documented and in place to respond quickly to suspected or known security incidents, and to mitigate these to the extent practicable. Investigations and corrective action plans are fully documented.
10. Contingency Plan - 164.308(a)(7)(i)
    a. The practice's contingency plan is reviewed and tested on at least an annual basis and as needed if changes occur.
    b. Routine back up of company servers is in place where ephi resides.
    c. Formal system to track the receipt, manipulation, storage, dissemination, transmission and disposal of EPHI to ensure security is in place.
    d. The Designated Security Official conducts and oversees back ups
    e. Off Site Storage of backups is in place-INSERT DETAILS
    f. A Log of backups is maintained
    g. A Disaster Recovery Plan is in place to respond to computer system emergency or failure

h. Routine review of contingency plan is in place – INSERT DETAILS
i. Emergency power supply for company servers and computers is in place
j. Access to EPHI during emergency mode- Paper access would be available in emergency mode but not electronic access.
k. Identification of critical systems has been completed by Security Official and network diagram completed. Emergency mode policy is in place.

11. Evaluation- 164.308(a)(8)(i)
    a. Regular audit of practice's computer system records
    b. Policies and procedures review
    c. Frequency of policy review - monthly or when changes are made
12. Business Associate Agreements 164.308(b)(1)
    a. The Privacy Security Official has completed checks to ensure that routine changes, including upgrades, testing and maintenance do not compromise security
    b. Contracts and BAAs are in place for each business associate with whom it electronically shares EPHI
    c. A current list of BAAs and level of access is available
13. Facility Access Controls – 164.310(a)(1)
    a. The practice has a contingency plan for computer system emergencies and natural disasters- refer to policy
    b. Practice computer servers-INSERT DETAILS
    c. Practice remote locations – INSERT DETAILS
    d. There is a process in place to recover lost data from each work station- INSERT DETAILS.
    e. Practice is located in a medical complex building with other medical practices and other business offices – INSERT DETAILS
    f. There is a plan in place to ensure protection of exterior and interior of the practice and building from unauthorized physical access
    g. Security Guard- INSERT DETAILS
    h. Visitor Sign in Sheet- this is in place at the practice
    i. Log of repairs and modifications to physical components of the office is maintained by our HR Manger in conjunction with INSERT DETAILS, our building landlord.
14. Work Station Use and Security – 164.310(b-C)
    a. Work stations are not routinely shared; however, in the event this is needed, all staff and temporary employees utilize individual passwords
    b. Staff and physicians do not install or remove software from the practice.
    c. Laptops are available and require individual log on

d. iPhones are used and security measures are in place to ensure ePHI is protected
e. Work stations are locked and secure

15. Device and Media Controls – 164.310(d)(1)
    a. Polices are in place to merge duplicate patient records, and to make patient accounts inactive, but the practice does not destroy any computerized patient records. After at least seven years, the practice may initiate requests to destroy paper medical records after thorough review, approval and sign off.
    b. There is a system in place to track the receipt, manipulation, storage, dissemination, transmission and disposal of EPHI to ensure security, specifically, this addresses the retirement of devices that are no longer used. Data is wiped clean if possible from the hard drives as part of this process. Physical destruction of the hard drive is required.
    c. Policy on bringing hardware and software into the practice- Bring Your Own Device Policy
    d. Policy to ensure EPHI is not altered or destroyed by an unauthorized user- See Integrity policy as part of this.
    e. Written policy to connect new computer equipment and load new computer programs
    f. The practice has the ability to re-use disks, tapes and CDs- the Privacy Official oversees this process to ensure ePHI is removed before new use occurs
    g. Period review and documentation of maintenance on computer hard drives is completed.
    h. Log of repairs and modification of office physical components are maintained via work order requests that are submitted to INSERT DETAILS, our landlord.
    i. Inventory of work stations- hardware and software is maintained
    j. Policy on staff bringing device in from home- See Bring Your Own Device Policy- this is not allowed
    k. Routine back up on each practice work station is not required as ephi and company data resides on servers which are already backed up daily Monday thru Friday.
16. Access Control – 164.312(a)(1)
    a. Unique user id for each employee is in place
    b. Minimal access for users via set procedures is practiced
    c. Access to ePHI during an emergency- See Break the Glass Policy
    d. Automatic log off set up for set time frame- in place

i. Pass word protection feature- in place

e. Transmission of EPHI via communication network is in place

f. Use of technology to ensure message received matches message sent is in place

17. Audit Controls – 164.312(b)
    a. There is a process set up to account for all activity related to ePHI- addition/removal of software/hardware, passwords, access and security incidents
18. Integrity – 164.312©(1)
    a. Procedure to protect ePHI from being altered or destroyed
19. Person or Entity Authentication – 164.312(d)
    a. Computers have built in security features where needed –
        i. Passwords
        ii. Encryption
        iii. Automatic screen savers
20. Transmission Security
    a. Server access via modem connection is available
    b. Local area network is operated at the practice
    c. Wide area network – The practice does not operate a WAN. The practice does connect to the Internet for access to encrypted sites, VPNs, research, etc.
    d. Virtual Private Network (VPN) - multiple VPN connections are used.
    e. Encryption Technology is in place
    f. Fax Capability is in place
    g. Encryption Software is in place- Please refer to Encryption Policy. We have addressed laptops, backups and https for access to interfaces INSERT DETAILS

<u>Items to Implement</u> – INSERT DETAILS ON ITEMS Completed:

<u>Items to Consider for Implementation</u> – INSERT DETAILS

<u>CURRENT Items to Implement: INSERT DETAILS</u>