a.

HIPAA RISK ANALYSIS and MANAGEMENT TOOL

Electronic Devices and Systems

Device or System: _____

Physical Location: Green Hills (main office, satellite, etc.)
Direct Family Care - Main office

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Potential Threat or Vulnerability	**Yes/No**	**Related Policy # (Required or Addressable)**	**Likelihood of Occurrence (0-5)**	**Impact to EPHI (0-5)**	**Total Risk Level (#4 x #5)**	**Possible Solutions**	**Date Implemented**
Remote Access							
Can employees access ePHI from home or other remote locations?	Yes	5 (A)					
Do employees save ePHI on diskettes or CDs for use on their home computer?	No	6 (A)					
Do employees use other mobile devices to access ePHI?	Yes	6 (A)					
Passwords/Logins							
Is access limited to only those employees who need it to perform their job?	Yes	4 (A)					
Are there unique logons and passwords for all who access ePHI?	Yes	15 (R)					
Are logons and passwords logged in the event a user loses or forgets their ID?	No	5 (A)					

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Potential Threat or Vulnerability	**Yes/No**	**Related Policy # (Required or Addressable)**	**Likelihood of Occurrence (0-5)**	**Impact to EPHI (0-5)**	**Total Risk Level (#4 x #5)**	**Possible Solutions**	**Date Implemented**
Are login attempts limited (i.e., three unsuccessful attempts will trigger system lock)?	Yes	6 (A)					
Do employees share passwords?	No	6 (A)					
Is each user assigned the appropriate level of access?	Yes	5 (A)					
Are access levels changed/modified when a user's employment status changes?	Yes	5 (A)					
Is all access removed when an employee terminates?	Yes	4 (A)					
Are passwords changed periodically?	Yes	6 (A)					
Are password standards required (i.e. minimum length, mix of characters, etc.)?	Yes	6 (A)					
Access by External or Unauthorized Parties							
Do any outside parties have access to this device/system?	Yes	5 (A)					
Does the practice utilize an outside IT vendor to support this device/system?	Yes	5 (A)					
Does an independent contractor use this device/system (transcription service, management company, temp service, etc.)?	No	5 (A)					

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Potential Threat or Vulnerability	**Yes/No**	**Related Policy # (Required or Addressable)**	**Likelihood of Occurrence (0-5)**	**Impact to EPHI (0-5)**	**Total Risk Level (#4 x #5)**	**Possible Solutions**	**Date Implemented**
Is the computer left on after office hours or during unsupervised periods?	No	12 (R)					
Is the screen visible to persons unauthorized to access ePHI?	No	12 (R)					
Do you utilize automatic logoff when computers have been idle for a specified period of time?	Yes	15 (A)					
Do you transport PHI or ePHI outside the facility?	Yes	12 (R)					
Do you utilize password-enabled screen savers?	Yes	13 (R)					
Virus Protection							
Is virus protection software utilized?	Yes	17 (A)					
Is virus protection software updated regularly?	Yes	17 (A)					
Do you scan computers for viruses on a regular basis?	Yes	17 (A)					
Maintenance							
Is hardware and software maintenance logged?	Yes	14 (A)					
Do you log occasions when hardware is moved?	Yes	14 (A)					
Workstation Use							
Do you have a policy specifying which functions may or may not be performed on the workstation?	Yes	12 (R)					

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Potential Threat or Vulnerability	**Yes/No**	**Related Policy # (Required or Addressable)**	**Likelihood of Occurrence (0-5)**	**Impact to EPHI (0-5)**	**Total Risk Level (#4 x #5)**	**Possible Solutions**	**Date Implemented**
Do you have a policy specifying the manner in which these functions are to be performed?	Yes	12 (R)					
Do you have a policy specifying the physical attributes of the workstation (i.e. privacy, proximity of liquids, etc.)?	Yes	12 (R)					
Do you have a policy for requesting hardware or software changes to a workstation?	Yes	14 (A)					
Security Incident Procedures							
Are employees trained on what constitutes a security incident and how to report it?	Yes	6 (A)					
Are security incidents monitored and logged?	Yes	7 (R)					
Backup							
Do you backup ePHI daily?	Yes	8 (R)					
Does your daily backup include only file changes?	No	8 (R)					
Do you do a full backup (all files) regularly?	Yes	8 (R)					
Do you perform a bootable (image-based) backup regularly?		8 (R)					
Do you keep any backup media offsite?	Yes	14 (A)					
Do you alternate backup media?	Yes	8 (R)					

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Potential Threat or Vulnerability	**Yes/No**	**Related Policy # (Required or Addressable)**	**Likelihood of Occurrence (0-5)**	**Impact to EPHI (0-5)**	**Total Risk Level (#4 x #5)**	**Possible Solutions**	**Date Implemented**
Are changes to ePHI logged by date and user?	Yes	16 (R)					
Is your backup password protected?	Yes	8 (R)					
Do you have copies of all software programs offsite?	Yes	14 (A)					
Do you use an outside service for off-site storage of backup media?	Yes	8 (R)					
Do you perform online backups?	Yes	8 (R)					
Do you test your backups periodically?	Yes	8 (R)					
Internet/Email							
Do you use this device/system to access the Internet?	Yes	12 (R)					
Do users download Internet files or install personal software?	No	6 (A)					
Do you use e-mail to transmit ePHI?	Yes	19 (A)					
Do you utilize encryption for e-mail containing ePHI?	Yes	15 (A)					
If patients send you e-mail containing ePHI, have you advised them of the risks involved?	Yes	19 (A)					
Media (tapes, diskettes, CDs, etc.)							
Are media containing ePHI destroyed prior to being discarded?	Yes	14 (R)					
Do you use tapes for transcription?	No	14 (R)					

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Potential Threat or Vulnerability	**Yes/No**	**Related Policy # (Required or Addressable)**	**Likelihood of Occurrence (0-5)**	**Impact to EPHI (0-5)**	**Total Risk Level (#4 x #5)**	**Possible Solutions**	**Date Implemented**
Are tapes erased after transcription has been proofread and signed?	n/a	14 (R)					
Is all ePHI removed from media before it is reused (excluding backup media)?	n/a	14 (R)					
Audit Controls							
Do you record logins to devices or software containing ePHI?	Yes	16 (R)					
Is login activity monitored and reviewed periodically?	Yes	16 (R)					
Integrity							
Do you have policies to protect ePHI from unauthorized changes?	Yes	15 (R)					
Do you have electronic mechanisms to corroborate that ePHI has not been changed?	Yes	17 (A)					
Person or Entity Authentication							
Do you have procedures to verify the identity of persons seeking access to ePHI?	Yes	18 (R)					
Business Associate Agreements							
Is there a vendor relationship with this device or system that would require a BAA?	Yes	10 (R)					

Susan Lee 7/11/16