Vendor Management

“Getting Ready to Hit the Trail…or, hit the dust…”

BY: **THOMAS MILLER, MA, LPC, ALPS, ADC**

PRIVACY & SECURITY OFFICER

WEST VIRGINIA DEPARTMENT OF ADMINISTRATION

FOR THE 2018 NATIONAL HIPAA SUMMIT – ALEXANDRIA, VIRGINIA

"Your mission, should you choose to accept it, is to stay off of the OCR's, 'naughty list…' and out of a court room…"

“It is a lot easier to get into the swamp then get out of the swamp…” – Mark Twain

Good vendor management…

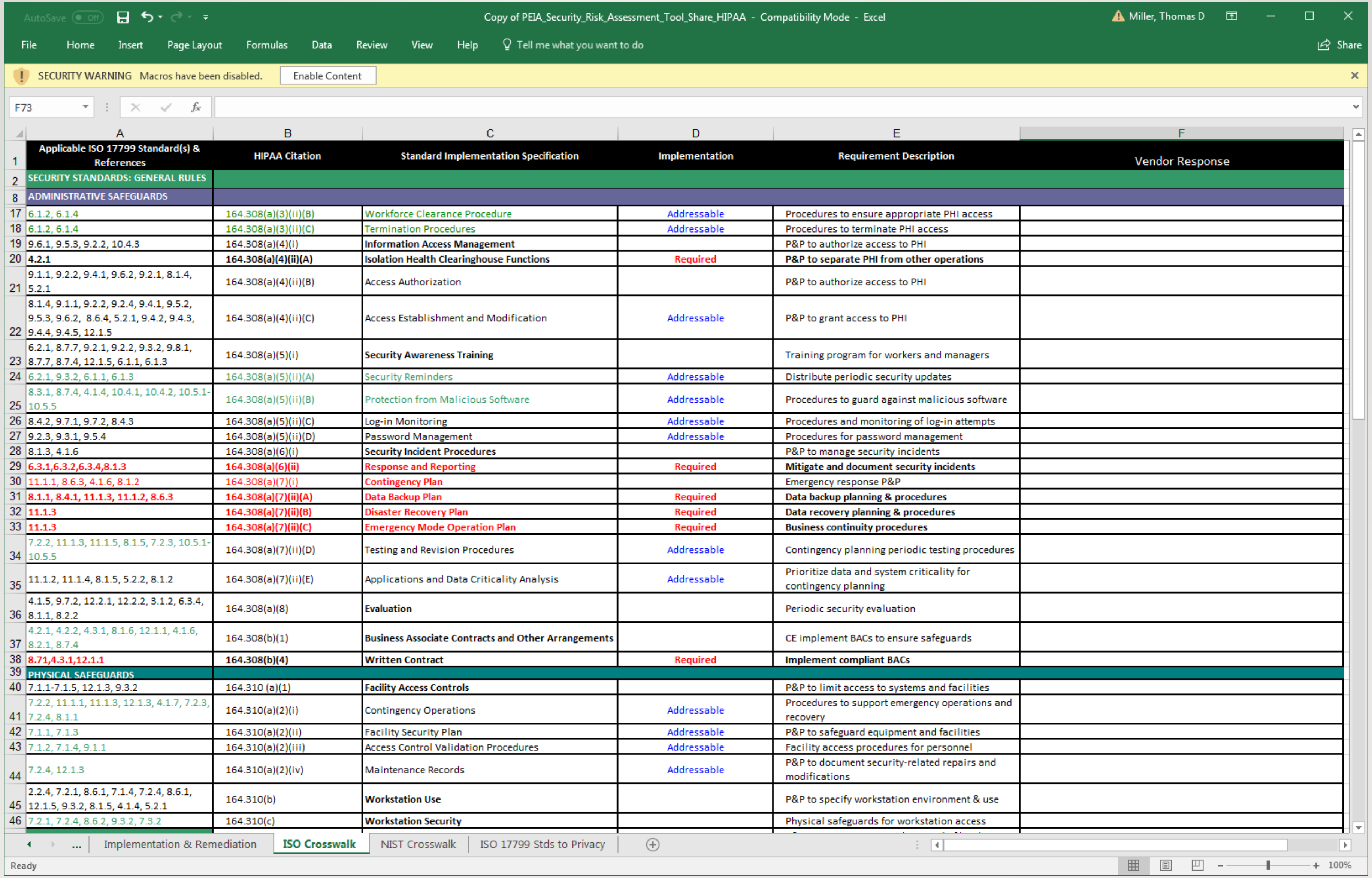
- Begins with solid polices and procedures
- Begins before any RFP, RFQ, or procurement
- Begins with the project design
- Must have a process
- Must have a plan
- Must be applied consistently

Good vendor management…

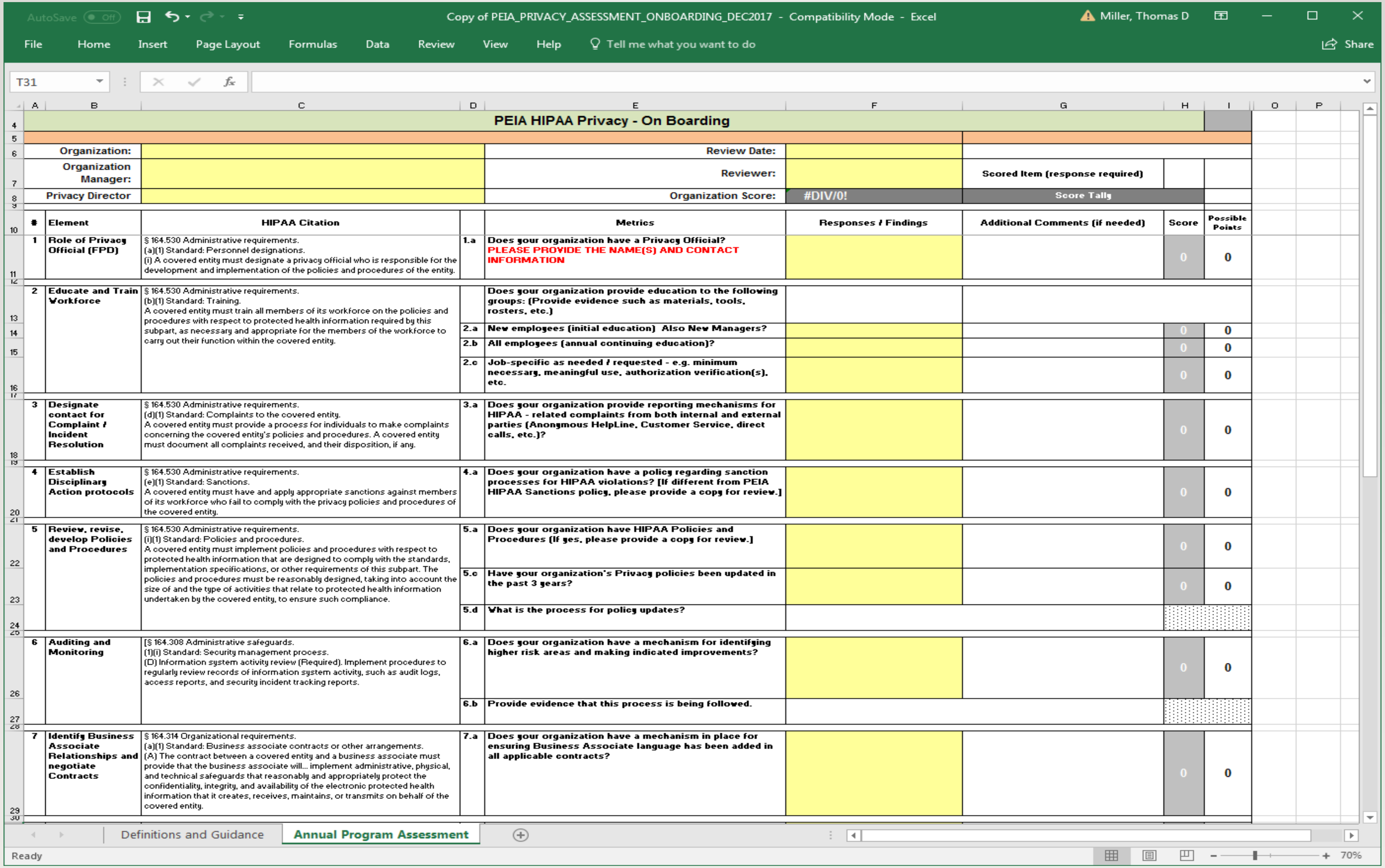
- Knowing what data you have – where it is - and when it got there, and when and how it will be disposed of
- Asserting ownership over your data – both in identifiable and de-identified formats
- Being able to track your data "…cradle to grave"
- Having clear vendor expectations in contract language – "Performance Guarantees"
- Tracking contracts, BAAs, Agreements, renewals, modifications, etc.
- Driving terms and conditions of contracts, BAAs, Agreements down to any and/or all subcontractors

Performing “Vendor Assurances”…

- Begins with the project planning
- Must be clear in RFPs/RFQs, contracts, and Agreements
  - “Onboarding”
  - Privacy & Security contacts must be identified
  - Data control – “No data may leave the Continental United States…”
- Use of Tools – Grids, cross-walks, etc. (HIPAA, NIST, ISO, SAS 70/SSAE 16/SOC, etc.)
- Breach Insurance requirement(s) – naming you as a co-insured


AutoSave Off
Copy of PEIA_Security_Risk_Assessment_Tool_Share_HIPAA - Compatibility Mode - Excel
Miller, Thomas D
Share
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Tell me what you want to do
SECURITY WARNING Macros have been disabled.
Enable Content
F73
Implementation & Remediation
ISO Crosswalk
NIST Crosswalk
ISO 17799 Stds to Privacy
Ready
100%

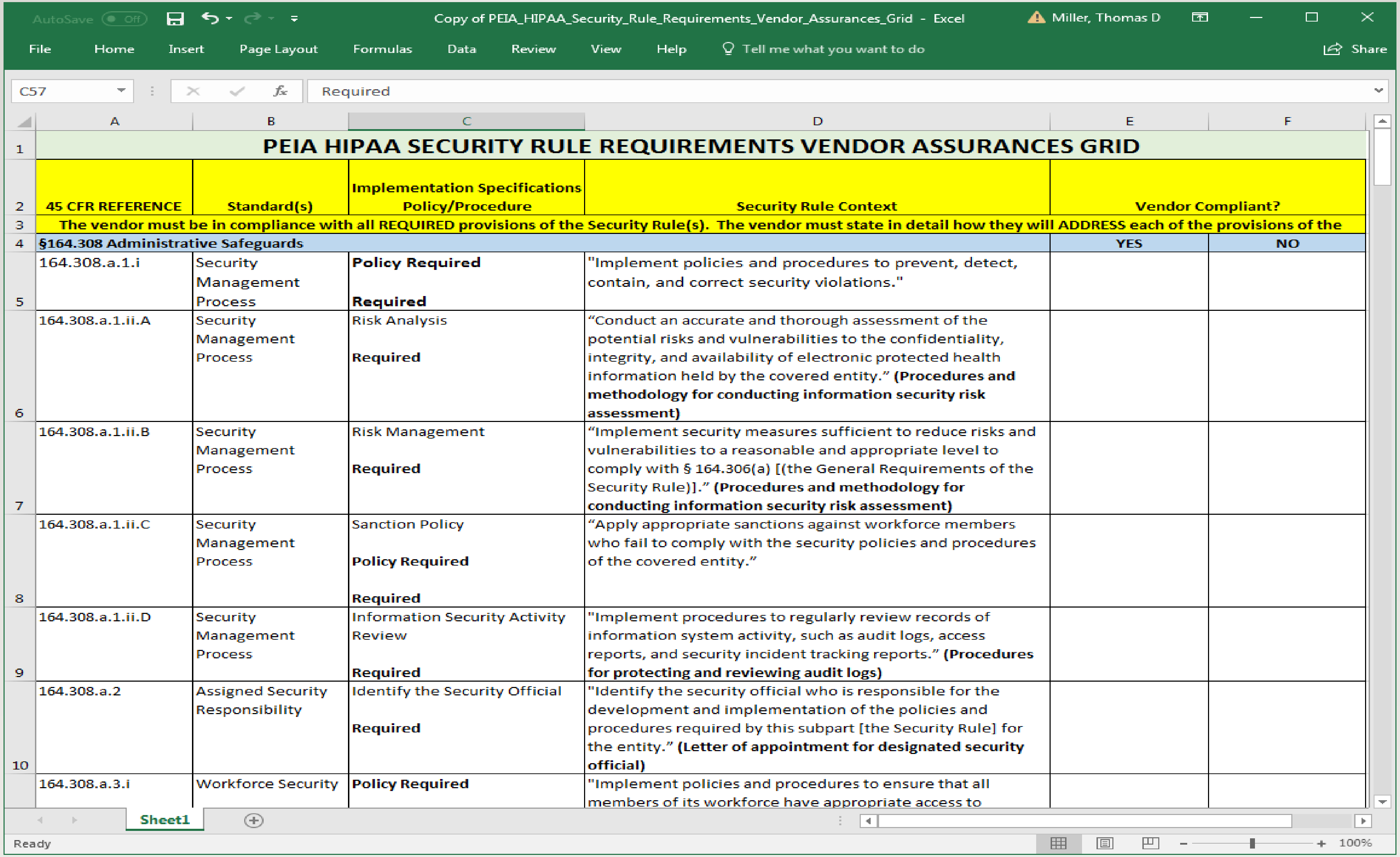
	A	B	C	D	E	F
1	Applicable ISO 17799 Standard(s) & References	HIPAA Citation	Standard Implementation Specification	Implementation	Requirement Description	Vendor Response
2	SECURITY STANDARDS: GENERAL RULES					
8	ADMINISTRATIVE SAFEGUARDS					
17	6.1.2, 6.1.4	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PHI access	
18	6.1.2, 6.1.4	164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	Procedures to terminate PHI access	
19	9.6.1, 9.5.3, 9.2.2, 10.4.3	164.308(a)(4)(i)	**Information Access Management**		P&P to authorize access to PHI	
20	**4.2.1**	**164.308(a)(4)(ii)(A)**	**Isolation Health Clearinghouse Functions**	Required	**P&P to separate PHI from other operations**	
21	9.1.1, 9.2.2, 9.4.1, 9.6.2, 9.2.1, 8.1.4, 5.2.1	164.308(a)(4)(ii)(B)	Access Authorization		P&P to authorize access to PHI	
22	8.1.4, 9.1.1, 9.2.2, 9.2.4, 9.4.1, 9.5.2, 9.5.3, 9.6.2, 8.6.4, 5.2.1, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 12.1.5	164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	P&P to grant access to PHI	
23	6.2.1, 8.7.7, 9.2.1, 9.2.2, 9.3.2, 9.8.1, 8.7.7, 8.7.4, 12.1.5, 6.1.1, 6.1.3	164.308(a)(5)(i)	**Security Awareness Training**		Training program for workers and managers	
24	6.2.1, 9.3.2, 6.1.1, 6.1.3	164.308(a)(5)(ii)(A)	Security Reminders	Addressable	Distribute periodic security updates	
25	8.3.1, 8.7.4, 4.1.4, 10.4.1, 10.4.2, 10.5.1-10.5.5	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Addressable	Procedures to guard against malicious software	
26	8.4.2, 9.7.1, 9.7.2, 8.4.3	164.308(a)(5)(ii)(C)	Log-in Monitoring	Addressable	Procedures and monitoring of log-in attempts	
27	9.2.3, 9.3.1, 9.5.4	164.308(a)(5)(ii)(D)	Password Management	Addressable	Procedures for password management	
28	8.1.3, 4.1.6	164.308(a)(6)(i)	**Security Incident Procedures**		P&P to manage security incidents	
29	**6.3.1,6.3.2,6.3.4,8.1.3**	**164.308(a)(6)(ii)**	**Response and Reporting**	Required	**Mitigate and document security incidents**	
30	11.1.1, 8.6.3, 4.1.6, 8.1.2	164.308(a)(7)(i)	**Contingency Plan**		Emergency response P&P	
31	**8.1.1, 8.4.1, 11.1.3, 11.1.2, 8.6.3**	**164.308(a)(7)(ii)(A)**	**Data Backup Plan**	Required	**Data backup planning & procedures**	
32	**11.1.3**	**164.308(a)(7)(ii)(B)**	**Disaster Recovery Plan**	Required	**Data recovery planning & procedures**	
33	**11.1.3**	**164.308(a)(7)(ii)(C)**	**Emergency Mode Operation Plan**	Required	**Business continuity procedures**	
34	7.2.2, 11.1.3, 11.1.5, 8.1.5, 7.2.3, 10.5.1-10.5.5	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Addressable	Contingency planning periodic testing procedures	
35	11.1.2, 11.1.4, 8.1.5, 5.2.2, 8.1.2	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Addressable	Prioritize data and system criticality for contingency planning	
36	4.1.5, 9.7.2, 12.2.1, 12.2.2, 3.1.2, 6.3.4, 8.1.1, 8.2.2	164.308(a)(8)	**Evaluation**		Periodic security evaluation	
37	4.2.1, 4.2.2, 4.3.1, 8.1.6, 12.1.1, 4.1.6, 8.2.1, 8.7.4	164.308(b)(1)	**Business Associate Contracts and Other Arrangements**		CE implement BACs to ensure safeguards	
38	**8.71,4.3.1,12.1.1**	**164.308(b)(4)**	**Written Contract**	Required	**Implement compliant BACs**	
39	PHYSICAL SAFEGUARDS					
40	7.1.1-7.1.5, 12.1.3, 9.3.2	164.310 (a)(1)	**Facility Access Controls**		P&P to limit access to systems and facilities	
41	7.2.2, 11.1.1, 11.1.3, 12.1.3, 4.1.7, 7.2.3, 7.2.4, 8.1.1	164.310(a)(2)(i)	Contingency Operations	Addressable	Procedures to support emergency operations and recovery	
42	7.1.1, 7.1.3	164.310(a)(2)(ii)	Facility Security Plan	Addressable	P&P to safeguard equipment and facilities	
43	7.1.2, 7.1.4, 9.1.1	164.310(a)(2)(iii)	Access Control Validation Procedures	Addressable	Facility access procedures for personnel	
44	7.2.4, 12.1.3	164.310(a)(2)(iv)	Maintenance Records	Addressable	P&P to document security-related repairs and modifications	
45	2.2.4, 7.2.1, 8.6.1, 7.1.4, 7.2.4, 8.6.1, 12.1.5, 9.3.2, 8.1.5, 4.1.4, 5.2.1	164.310(b)	**Workstation Use**		P&P to specify workstation environment & use	
46	7.2.1, 7.2.4, 8.6.2, 9.3.2, 7.3.2	164.310(c)	**Workstation Security**		Physical safeguards for workstation access	


AutoSave Off
Copy of PEIA_PRIVACY_ASSESSMENT_ONBOARDING_DEC2017 - Compatibility Mode - Excel
Miller, Thomas D
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Tell me what you want to do
Share
T31
fx
Definitions and Guidance
Annual Program Assessment
Ready
70%

PEIA HIPAA Privacy - On Boarding

Organization:		Review Date:	
Organization Manager:		Reviewer:		Scored Item (response required)
Privacy Director		Organization Score:	#DIV/0!	Score Tally

#	Element	HIPAA Citation		Metrics	Responses / Findings	Additional Comments (if needed)	Score	Possible Points
1	Role of Privacy Official (FPD)	§ 164.530 Administrative requirements. (a)(1) Standard: Personnel designations. (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.	1.a	Does your organization have a Privacy Official? PLEASE PROVIDE THE NAME(S) AND CONTACT INFORMATION			0	0
2	Educate and Train Workforce	§ 164.530 Administrative requirements. (b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.		Does your organization provide education to the following groups: (Provide evidence such as materials, tools, rosters, etc.)				
			2.a	New employees (initial education) Also New Managers?			0	0
			2.b	All employees (annual continuing education)?			0	0
			2.c	Job-specific as needed / requested - e.g. minimum necessary, meaningful use, authorization verification(s), etc.			0	0
3	Designate contact for Complaint / Incident Resolution	§ 164.530 Administrative requirements. (d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures. A covered entity must document all complaints received, and their disposition, if any.	3.a	Does your organization provide reporting mechanisms for HIPAA - related complaints from both internal and external parties (Anonymous HelpLine, Customer Service, direct calls, etc.)?			0	0
4	Establish Disciplinary Action protocols	§ 164.530 Administrative requirements. (e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity.	4.a	Does your organization have a policy regarding sanction processes for HIPAA violations? [If different from PEIA HIPAA Sanctions policy, please provide a copy for review.]			0	0
5	Review, revise, develop Policies and Procedures	§ 164.530 Administrative requirements. (i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance.	5.a	Does your organization have HIPAA Policies and Procedures [If yes, please provide a copy for review.]			0	0
			5.c	Have your organization's Privacy policies been updated in the past 3 years?			0	0
			5.d	What is the process for policy updates?				
6	Auditing and Monitoring	[§ 164.308 Administrative safeguards. (1)(i) Standard: Security management process. (D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	6.a	Does your organization have a mechanism for identifying higher risk areas and making indicated improvements?			0	0
			6.b	Provide evidence that this process is being followed.				
7	Identify Business Associate Relationships and negotiate Contracts	§ 164.314 Organizational requirements. (a)(1) Standard: Business associate contracts or other arrangements. (A) The contract between a covered entity and a business associate must provide that the business associate will... implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity.	7.a	Does your organization have a mechanism in place for ensuring Business Associate language has been added in all applicable contracts?			0	0


AutoSave Off
Copy of PEIA_HIPAA_Security_Rule_Requirements_Vendor_Assurances_Grid - Excel
Miller, Thomas D
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Tell me what you want to do
Share
Sheet1
Ready
100%

C57 | Required

	A	B	C	D	E	F
1	PEIA HIPAA SECURITY RULE REQUIREMENTS VENDOR ASSURANCES GRID					
2	**45 CFR REFERENCE**	**Standard(s)**	**Implementation Specifications Policy/Procedure**	**Security Rule Context**	**Vendor Compliant?**	
3	**The vendor must be in compliance with all REQUIRED provisions of the Security Rule(s). The vendor must state in detail how they will ADDRESS each of the provisions of the**					
4	**§164.308 Administrative Safeguards**				**YES**	**NO**
5	164.308.a.1.i	Security Management Process	**Policy Required** **Required**	"Implement policies and procedures to prevent, detect, contain, and correct security violations."		
6	164.308.a.1.ii.A	Security Management Process	Risk Analysis **Required**	"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." **(Procedures and methodology for conducting information security risk assessment)**		
7	164.308.a.1.ii.B	Security Management Process	Risk Management **Required**	"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)]." **(Procedures and methodology for conducting information security risk assessment)**		
8	164.308.a.1.ii.C	Security Management Process	Sanction Policy **Policy Required** **Required**	"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."		
9	164.308.a.1.ii.D	Security Management Process	Information Security Activity Review **Required**	"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." **(Procedures for protecting and reviewing audit logs)**		
10	164.308.a.2	Assigned Security Responsibility	Identify the Security Official **Required**	"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity." **(Letter of appointment for designated security official)**		
	164.308.a.3.i	Workforce Security	**Policy Required**	"Implement policies and procedures to ensure that all members of its workforce have appropriate access to		

Questions, Comments, and/or Concerns…

Thomas D. Miller, MA, LPC, ALPS, ADC

Privacy & Security Officer

West Virginia Department of Administration

Public Employees Insurance Agency

601 57th Street, SE, Suite 2

Charleston, WV 25304

thomas.d.miller@wv.gov

304-558-7850, Ext. 52663