The Audits are here!

Janelle Burns, JD, CHPS – Janelle Burns Consulting, LLC

April Carlson, MBA, CFE, HCISPP – Privacy Officer, Mayo Clinic

The Audits were announced: Planning began at Baptist

- Review of the 419 page Audit Protocol
  - Particular attention to items of “documented evidence”
- Notification of senior management
- Notification of other departments whose assistance may be needed
- Notification of service lines
- Work with IT to ensure no OCR emails missed
- Repeat request for entities work on Business Associate spreadsheet

The Audits were announced: Mayo Clinic planning began

- #centralizeeverything
- Ensured BAAs were updated and scanned into centralized contracting system
- Notified twelve site/regional POs to forward all OCR emails to my attention for centralized response and tracking
- Worked with Information Security to ensure security risk assessments were documented, and finalized
- Continued to conduct random unannounced Privacy/Security site audits
- Prepared audit readiness SharePoint folder for all POs *(see example)*
  - Documented internal staff protocol for OCR onsite audits
  - Linked all supporting policies/procedures to Privacy Rule requirements by section

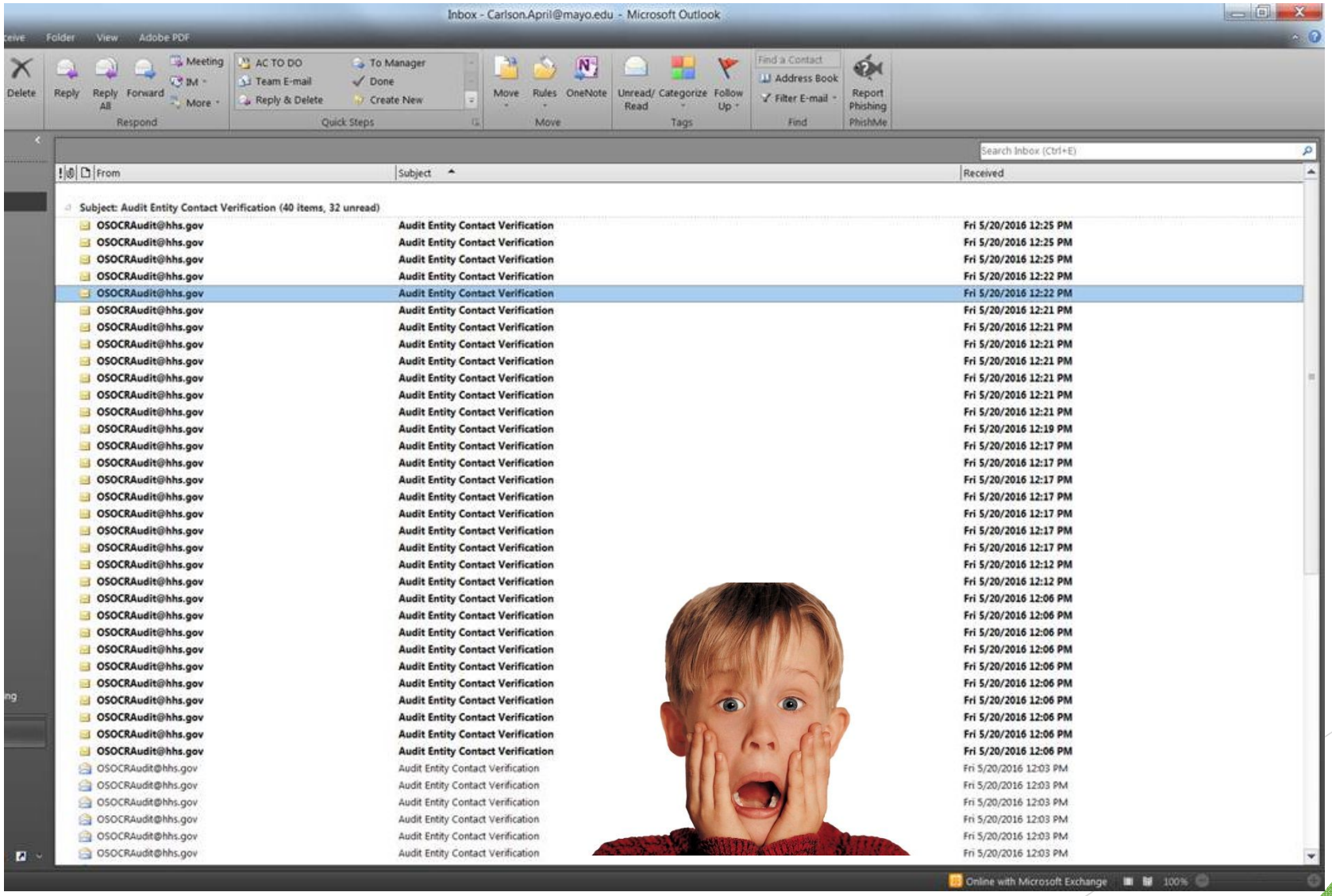
The Audits were announced: Mayo Clinic planning began *(examples)*

Section	Established Performance Criteria	Key Activity	Audit Procedures	HIPAA Compliance Area	Policy/Procedure Link	Review Date
§164.412	§164.412 If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	Law enforcement delay	Inquire of management as to how notifications are delayed in case of law enforcement requests. Obtain and review documentation of the process to delay notifications in case of law enforcement requests.	Breach	[link policy]	04/04/16
§164.502	§164.502 - Uses and disclosures of protected health information: general rules A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.	Deceased individuals	Inquire of management as to whether requirements with respect to PHI of a deceased person are met. Obtain and review the process and evaluate the content relative to the specified criteria used to ensure compliance with the requirements of PHI with respect to a deceased person.	Privacy	[link policy]	04/04/16

Baptist Nominations were received

- Waves of batched emails
- 55 emails in In Box upon return from lunch
- Work to de-duplicate
- Update senior management
- Re-submit answers for duplicates
- Touch base with administrative leader of each entity included in the auditee pool
  - Go over entity results of internal reviews
  - Offer support should entity be chosen for audit

Mayo Clinic Nominations were received:

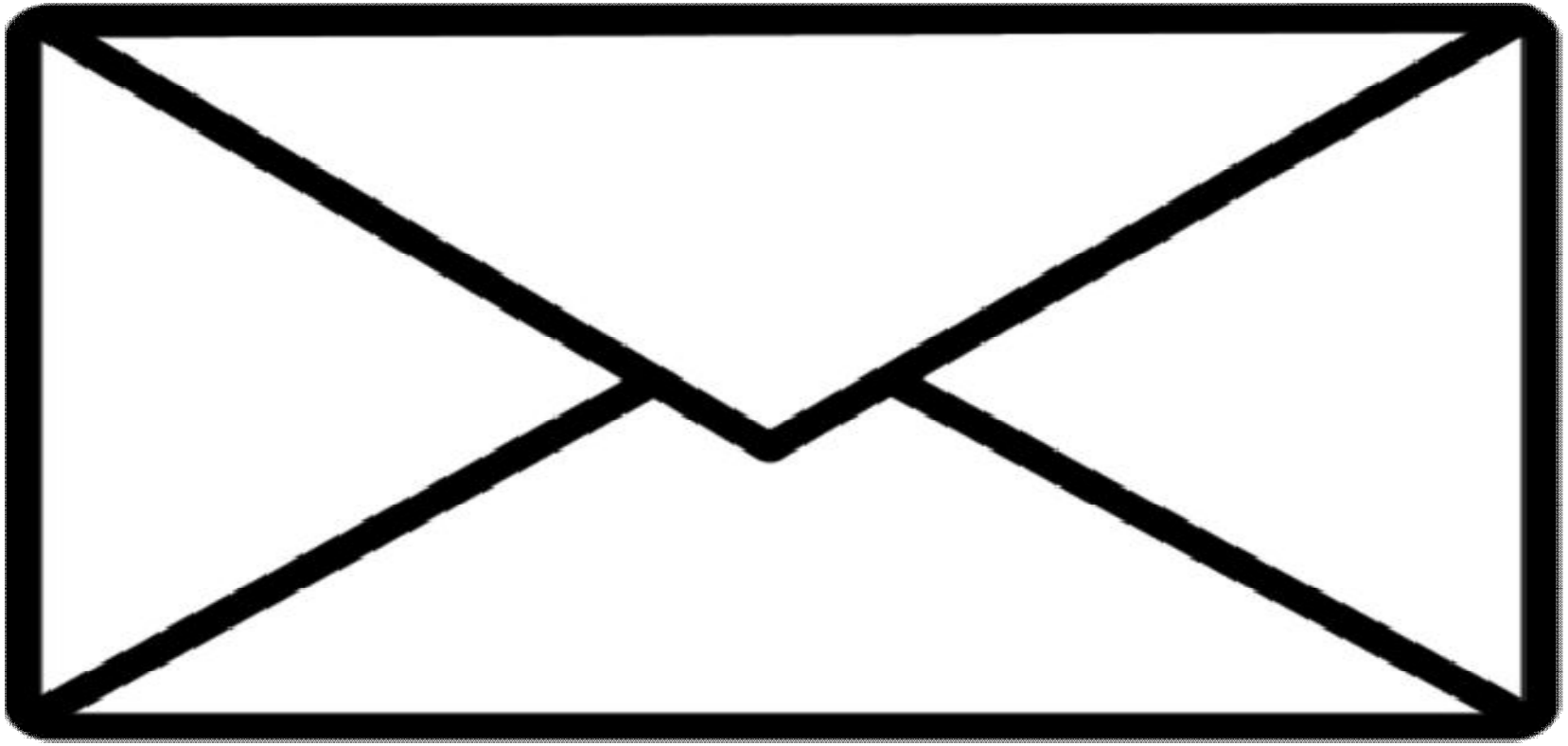


Questionnaire selection: 21 Mayo Clinic sites

- Immediately notified POs for selected entities to start gathering responses
- Created spreadsheet to provide standard template for responses
- Established clear timeline for site PO responses to allow time for Legal review and submission prior to deadline date in anticipation of system issues

Entity Name	Entity Address	Entity City	Entity State	Response4b	Response7	Response8	Response9	Response10	Response13
Mayo Clinic Health System - Red Cedar in Menomonie	2321 Stout Road	Menomonie	WI	Mayo Clinic and Mayo Clinic Health System – Eau Claire Hospital Inc. are joint members of Mayo Clinic Health System – Red Cedar in Menomonie	Tax exempt, nonprofit multidisciplinary group practice providing clinic and hospital patient care with programs in education and research.	106,848	27	82	$Revenue
Mayo Clinic Health System Home Health and Hospice	4033 123rd Street	Chippewa Falls	WI	Mayo Clinic is the sole member of Mayo Clinic Health System – Eau Claire Hospital Inc. Home Health and Hospice is a department of a non-profit, tax-exempt, acute care hospital.	As of 1/1/2015, Home Health and Hospice is operating as a department of MCHS – Eau Claire Hospital Inc. previously a separate entity.	38,491	0	434	$Revenue
Mayo Clinic Health System in St. James	1101 Moulton and Parsons Drive	St. James	MN	Mayo Clinic Health System—Mankato is the sole member of Mayo Clinic Health System-St. James	Tax exempt, nonprofit critical access hospital and clinic w/ emergency room	23,875	25	231	$Revenue
Mayo Clinic Health System – Chippewa Valley in Chippewa Falls	611 First Ave.	Chippewa Falls	WI	Mayo Clinic and Mayo Clinic Health System – Eau Claire Hospital Inc. are joint members of Mayo Clinic Health System – Chippewa Valley, Chippewa Falls location. Chippewa Falls Clinic is a regional clinic that collaborates with Mayo Clinic Health System – Chippewa Valley.	Tax exempt, nonprofit multidisciplinary group practice providing clinic patient care	18,053	0	207	$Revenue
Mayo Clinic Health System – Northland in Barron	1222 E. Woodland Ave., Suite C	Barron	WI	Mayo Clinic and Mayo Clinic Health System – Eau Claire Hospital Inc. are joint members of Mayo Clinic Health System – Northland in Barron, WI	Tax exempt, nonprofit multidisciplinary group practice providing clinic and hospital patient care with programs in education and research.	57,028	25	313	$Revenue

The Envelope, Please….



The Baptist Auditee is…..

- Immediately contact administrative leader of entity chosen
- Notify senior management
- Request assistance from other departments
- Help entity compile secondary contact information for BA list
- Participate in call facilitated by OCR

And the ONE Mayo Clinic Desk Auditee is…

- Immediately contacted site PO in La Crosse, WI
  - Did not receive Security risk assessment questions
- Notified senior management and Legal department
- Requested assistance from other departments (ROI, Legal, Contracting)
- BA list generated from centralized contract system (1500+)
- Participated in call facilitated by OCR
- Provided site PO with designated Senior Privacy Analyst to work with
- Established timeline to allow for Legal review and online system submission

Challenges for Baptist in Responding to Audit Questionnaire

- Records not kept in the format/manner OCR requested the information
- Difficulty in separating entity BAs from organization BAs
- Determining what documentation would be sufficient to satisfy OCR's request

Challenges with Mayo Clinic Responding to Audit Questionnaire

- BA system did not capture all of the OCR requested information
- Difficulty in separating single entity BAs from all Mayo Clinic BAs
- Working with ROI vendor (BA) added additional time and complexity to gather requested information
- Manual process for de-identification of samples
- Internal discussions and interpretation of what documentation was actually being requested

Compliance Effort OCR Ratings

Rating	Description
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.

Summary of Audit Ratings *(example)*

Rule	Element #, Section and Key Activity	Draft Rating
Breach	BNR12 §164.404(b) Timeliness of Notification	
Breach	BNR13 §164.404(c)(1) Content of Notification	
Privacy	P65 §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3) Right to access	
Privacy	P55 §164.520(a)(1) & (b)(1) Notice of Privacy Practices Content requirements	
Privacy	P58 §164.520(c)(3) Provision of Notice - Electronic Notice	

Detailed Analysis and Findings *(example)*

Element #	SECTION	KEY ACTIVITIES
BNR12	§164.404(b)	Timeliness of Notification
Preliminary Finding		
Preliminary Auditor Analysis		
Preliminary Rating		
Effect	Failure to provide a breach notification without reasonable delay or within 60 days of breach discovery may adversely impact the rights of the individuals who are subject to the breach.	

Lessons Learned:
What Mayo Clinic will change or do differently as a result of the audit

- Updated notification letter templates
- Implemented effective quality oversight of patient notification letters sent by site POs
- Updated 30 day extension letter for ROI
- Implemented effective quality oversight with ROI vendor (BA)
- Updated Notice of Privacy Practices
- Updated one policy to remove CLIA exception
- Worked with Public Affairs to move/change NPP link on all entity web pages to make the link more “prominent”
- Updated “required” fields in contract management system to align with OCR required reporting fields for BAAs

Additional Lessons Learned

- OCR's expectations for language in Notice may exceed actual wording of the regulations
  - More specifics about time periods for patient right of access, process for access, OCR address for complaints
- It is important to read OCR's draft findings carefully
  - There may be findings that can be refuted

Questions?