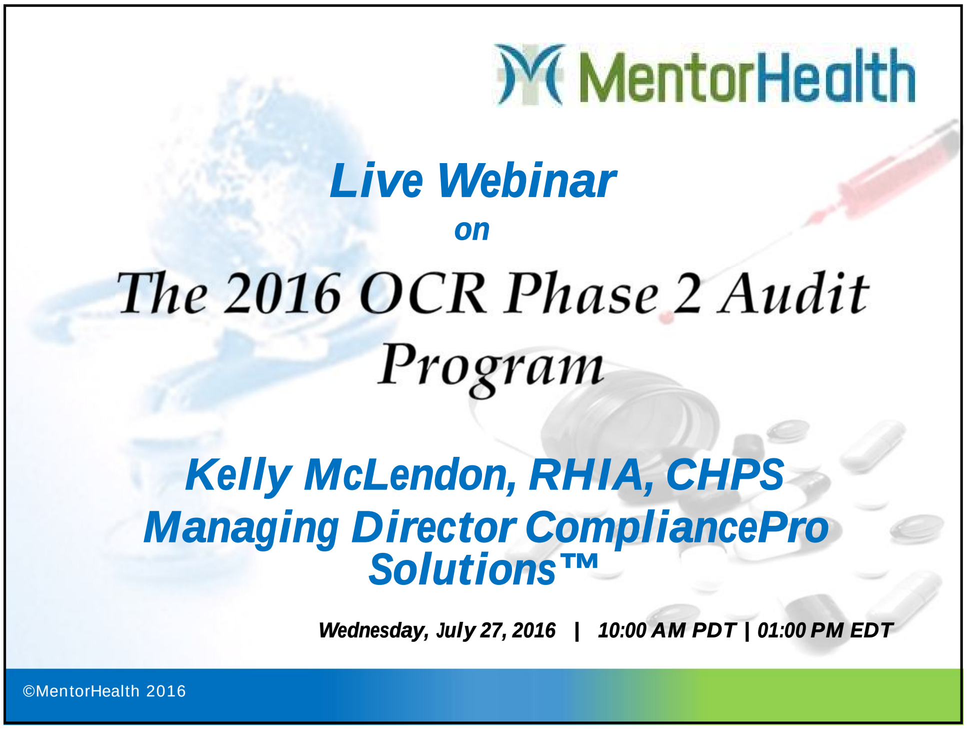


MentorHealth

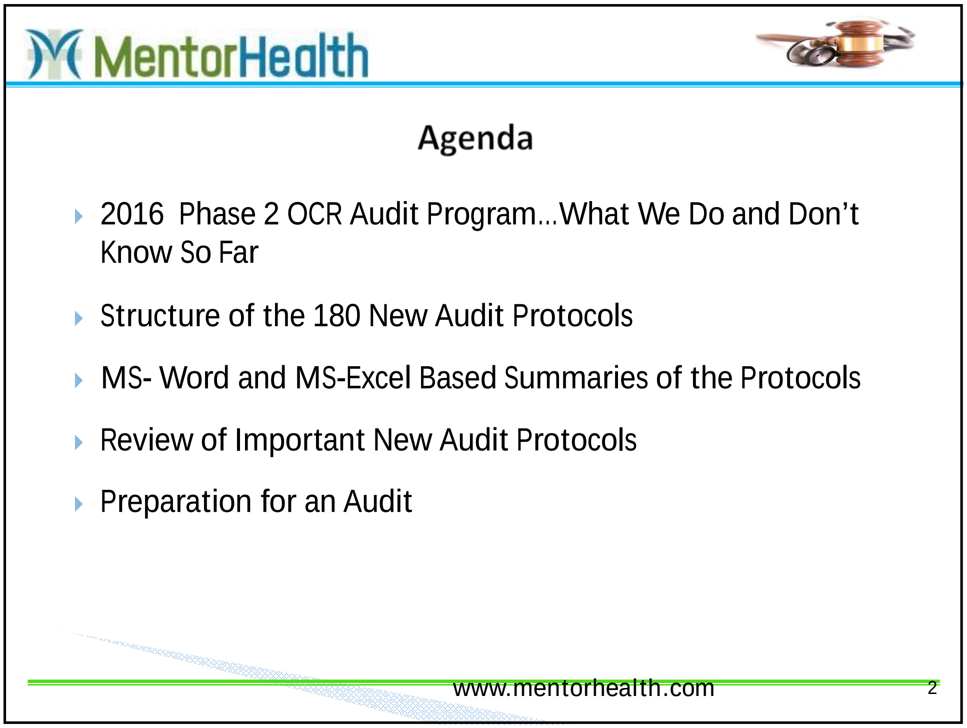
Live Webinar

on

The 2016 OCR Phase 2 Audit Program

Kelly McLendon, RHIA, CHPS
Managing Director CompliancePro Solutions™

Wednesday, July 27, 2016 | 10:00 AM PDT | 01:00 PM EDT

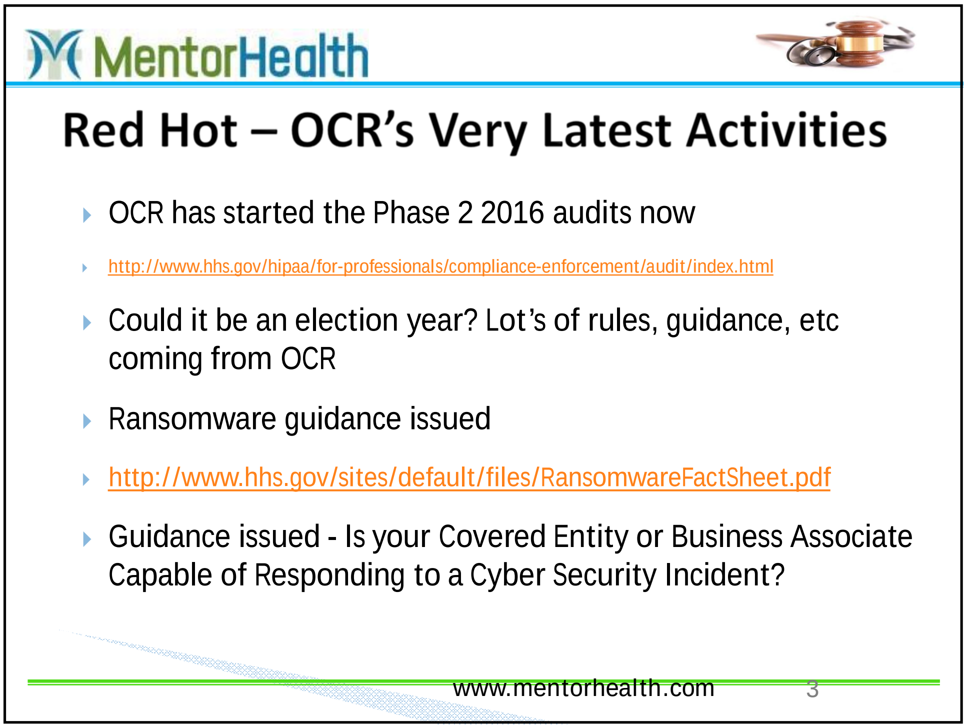


MentorHealth

Agenda

- 2016 Phase 2 OCR Audit Program…What We Do and Don't Know So Far
- Structure of the 180 New Audit Protocols
- MS- Word and MS-Excel Based Summaries of the Protocols
- Review of Important New Audit Protocols
- Preparation for an Audit

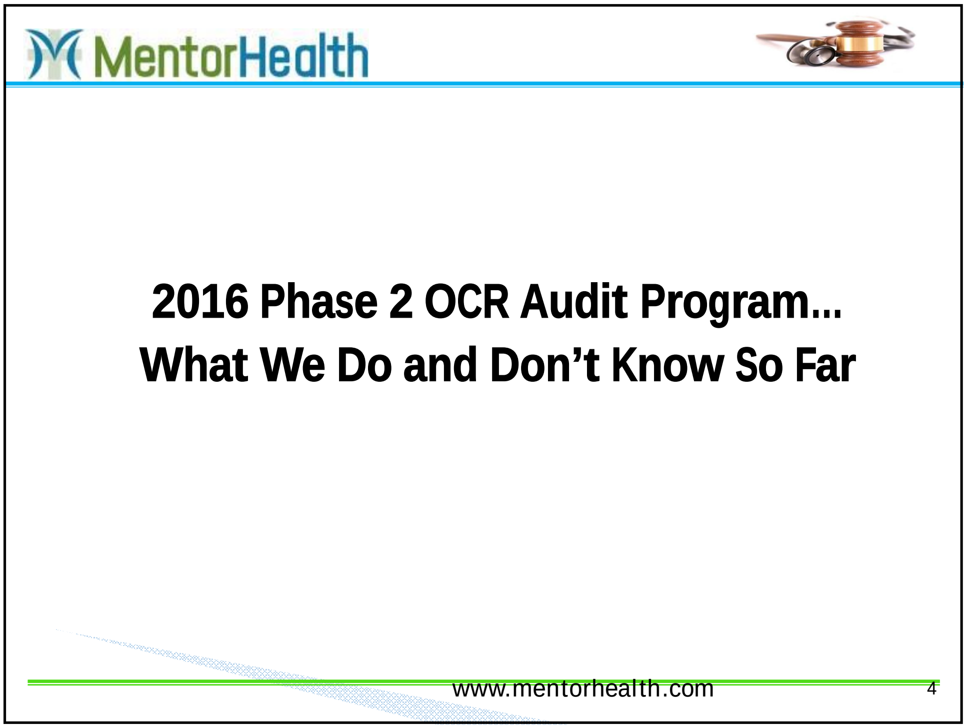
www.mentorhealth.com 2



MentorHealth

Red Hot – OCR's Very Latest Activities

- OCR has started the Phase 2 2016 audits now
- http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html
- Could it be an election year? Lot's of rules, guidance, etc coming from OCR
- Ransomware guidance issued
- http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- Guidance issued - Is your Covered Entity or Business Associate Capable of Responding to a Cyber Security Incident?

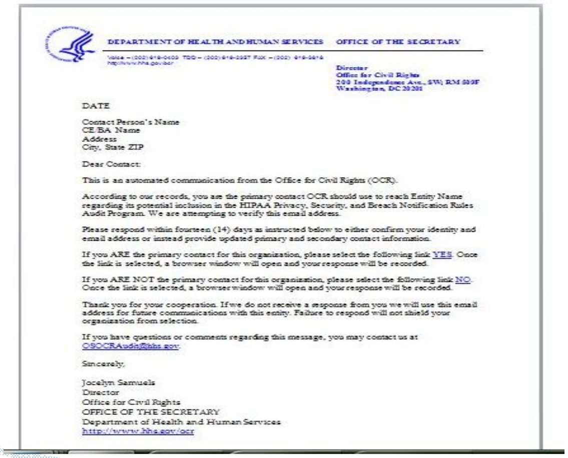


MentorHealth

2016 Phase 2 OCR Audit Program… What We Do and Don't Know So Far

MentorHealth

The Letter You Don’t Want to Get From OCR…Pre-Audit Contact Questions



DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice – (202) 619-0403 TDD – (202) 619-3257 FAX – (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

DATE

Contact Person’s Name
CE/BA Name
Address
City, State ZIP

Dear Contact:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach Entity Name regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

Sincerely,

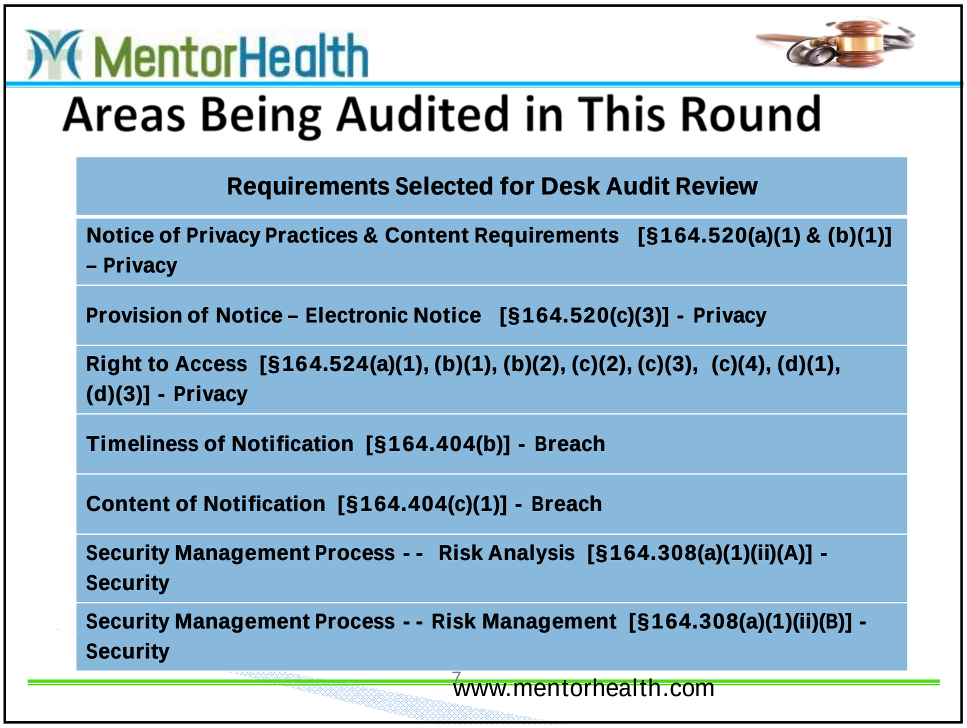
Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr

www.mentorhealth.com 5

MentorHealth

The New OCR Audits

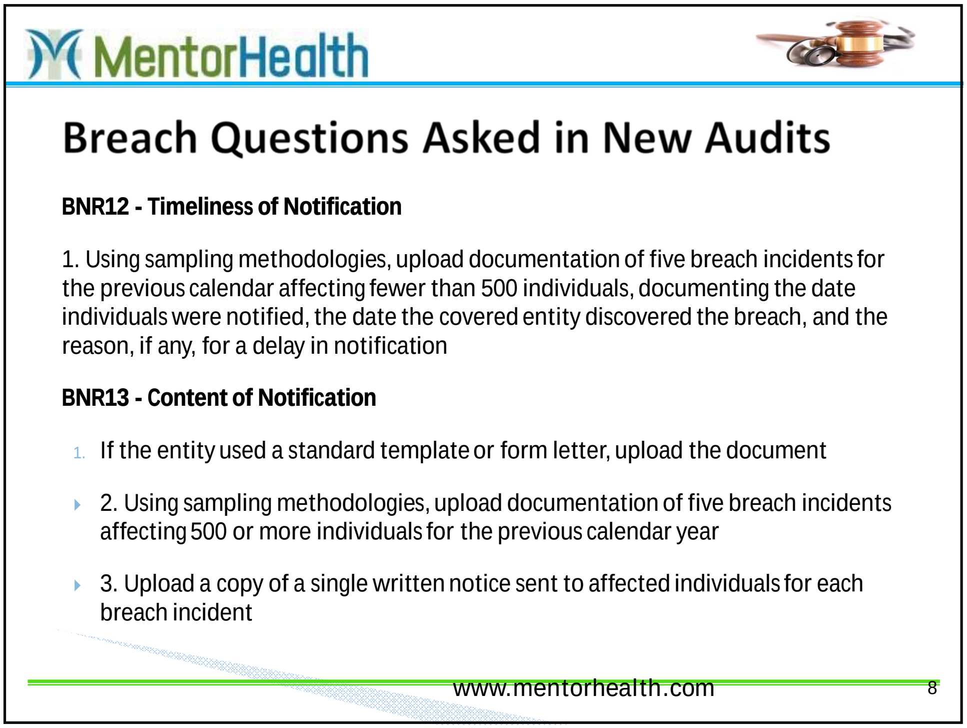
www.mentorhealth.com 6



MentorHealth

Areas Being Audited in This Round

Requirements Selected for Desk Audit Review
Notice of Privacy Practices & Content Requirements [§164.520(a)(1) & (b)(1)] – Privacy
Provision of Notice – Electronic Notice [§164.520(c)(3)] - Privacy
Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)] - Privacy
Timeliness of Notification [§164.404(b)] - Breach
Content of Notification [§164.404(c)(1)] - Breach
Security Management Process - - Risk Analysis [§164.308(a)(1)(ii)(A)] - Security
Security Management Process - - Risk Management [§164.308(a)(1)(ii)(B)] - Security



MentorHealth

Breach Questions Asked in New Audits

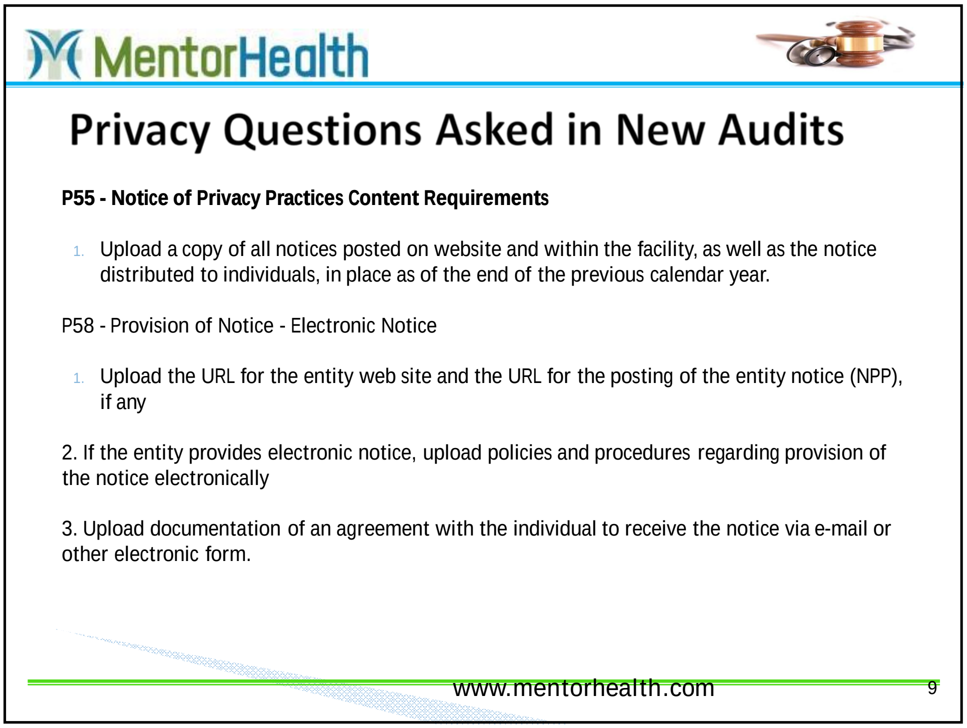
BNR12 - Timeliness of Notification

1. Using sampling methodologies, upload documentation of five breach incidents for the previous calendar affecting fewer than 500 individuals, documenting the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification

BNR13 - Content of Notification

1. If the entity used a standard template or form letter, upload the document

- 2. Using sampling methodologies, upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year
- 3. Upload a copy of a single written notice sent to affected individuals for each breach incident



Privacy Questions Asked in New Audits

P55 - Notice of Privacy Practices Content Requirements

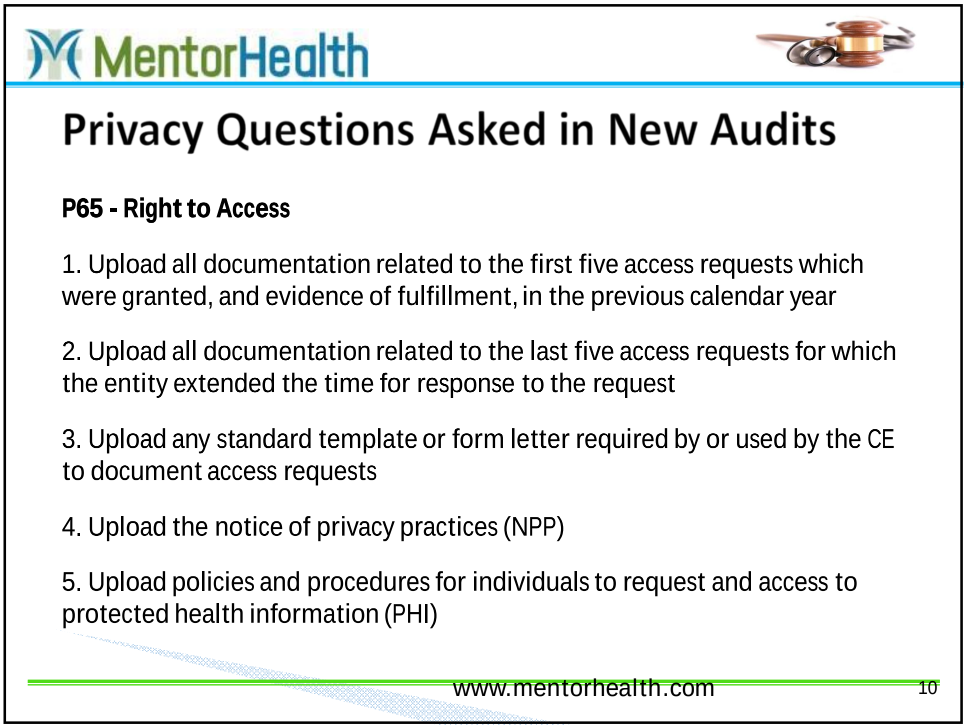
1. Upload a copy of all notices posted on website and within the facility, as well as the notice distributed to individuals, in place as of the end of the previous calendar year.

P58 - Provision of Notice - Electronic Notice

1. Upload the URL for the entity web site and the URL for the posting of the entity notice (NPP), if any

2. If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically

3. Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form.



Privacy Questions Asked in New Audits

P65 - Right to Access

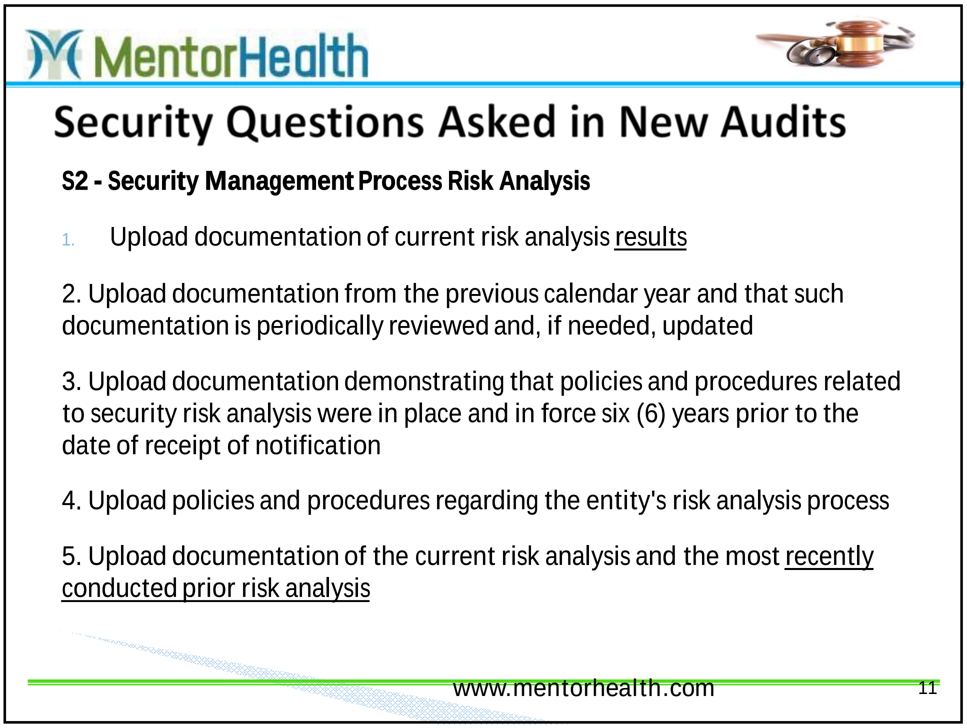
1. Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year

2. Upload all documentation related to the last five access requests for which the entity extended the time for response to the request

3. Upload any standard template or form letter required by or used by the CE to document access requests

4. Upload the notice of privacy practices (NPP)

5. Upload policies and procedures for individuals to request and access to protected health information (PHI)



MentorHealth

Security Questions Asked in New Audits

S2 - Security Management Process Risk Analysis

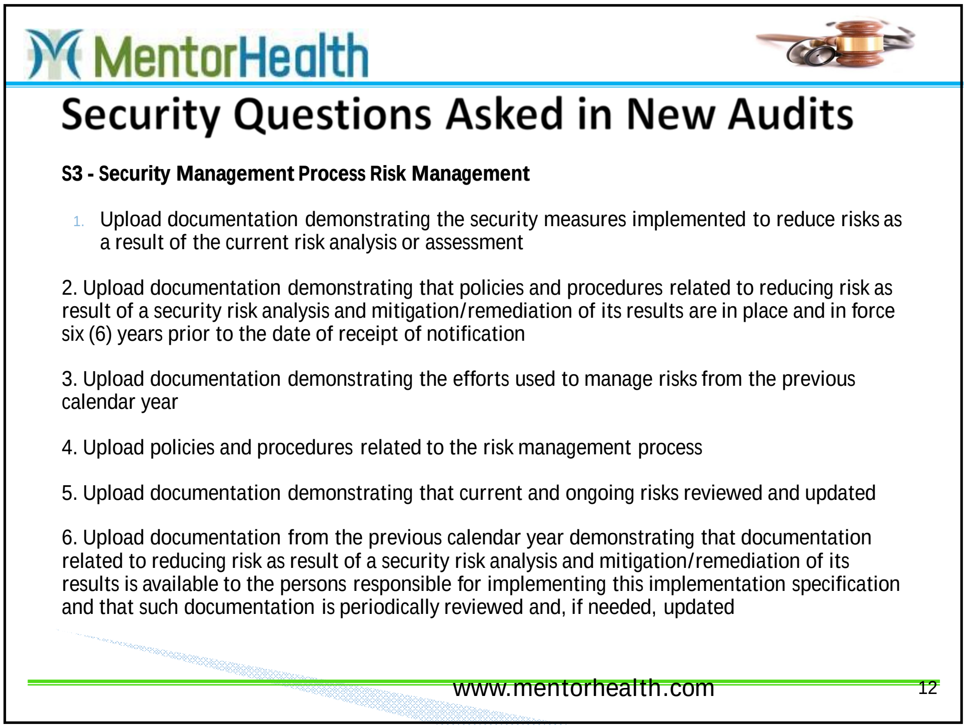
1. Upload documentation of current risk analysis results

2. Upload documentation from the previous calendar year and that such documentation is periodically reviewed and, if needed, updated

3. Upload documentation demonstrating that policies and procedures related to security risk analysis were in place and in force six (6) years prior to the date of receipt of notification

4. Upload policies and procedures regarding the entity's risk analysis process

5. Upload documentation of the current risk analysis and the most recently conducted prior risk analysis



MentorHealth

Security Questions Asked in New Audits

S3 - Security Management Process Risk Management

1. Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment

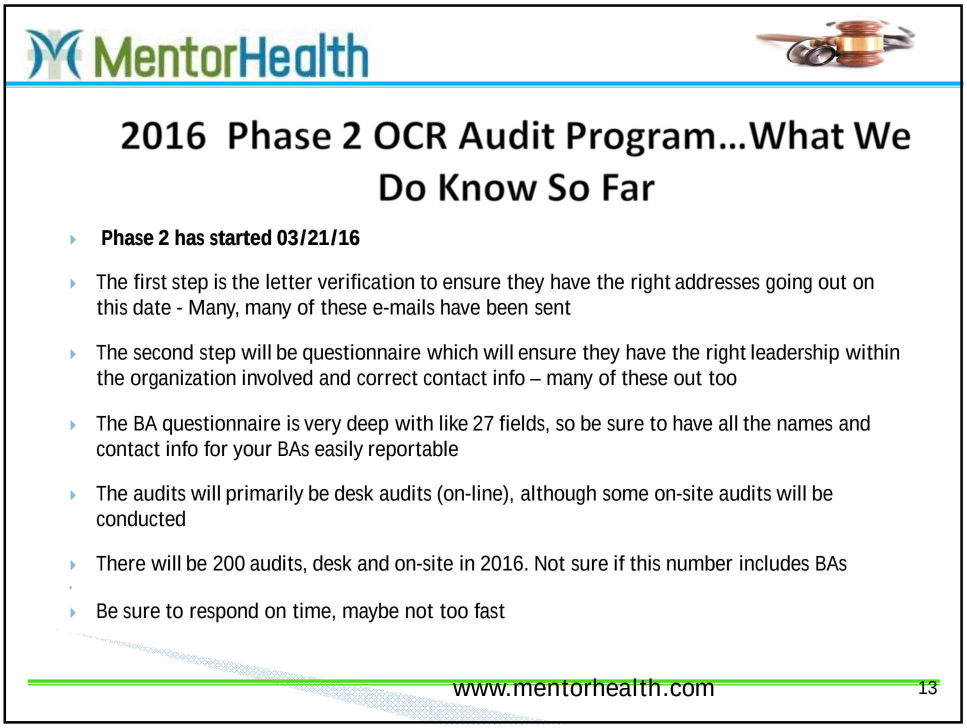
2. Upload documentation demonstrating that policies and procedures related to reducing risk as result of a security risk analysis and mitigation/remediation of its results are in place and in force six (6) years prior to the date of receipt of notification

3. Upload documentation demonstrating the efforts used to manage risks from the previous calendar year

4. Upload policies and procedures related to the risk management process

5. Upload documentation demonstrating that current and ongoing risks reviewed and updated

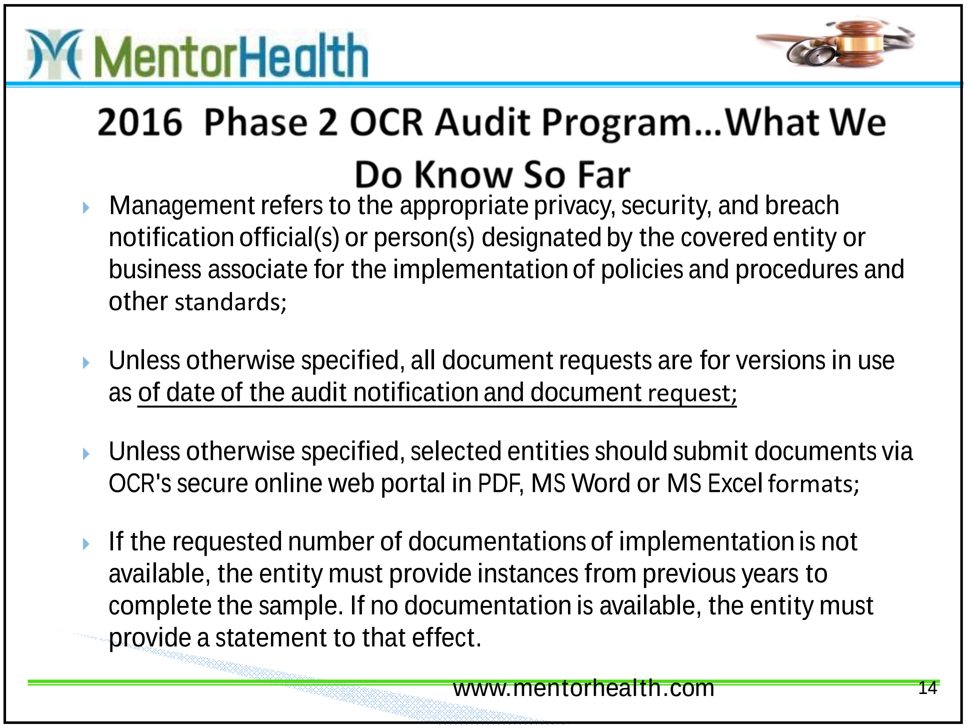
6. Upload documentation from the previous calendar year demonstrating that documentation related to reducing risk as result of a security risk analysis and mitigation/remediation of its results is available to the persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated



MentorHealth

2016 Phase 2 OCR Audit Program…What We Do Know So Far

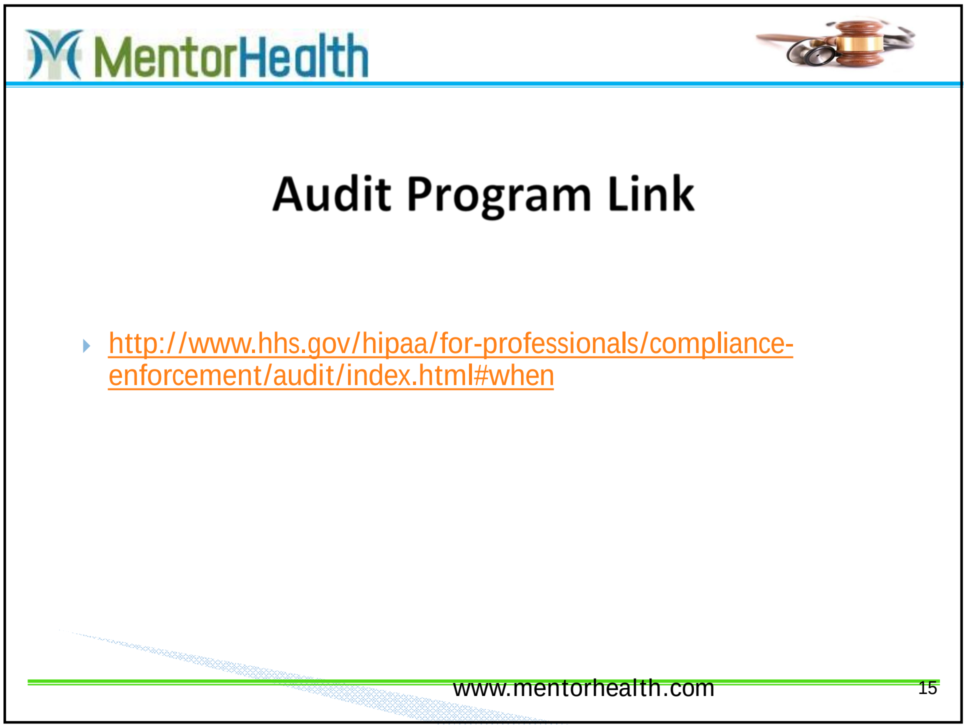
- **Phase 2 has started 03/21/16**
- The first step is the letter verification to ensure they have the right addresses going out on this date - Many, many of these e-mails have been sent
- The second step will be questionnaire which will ensure they have the right leadership within the organization involved and correct contact info – many of these out too
- The BA questionnaire is very deep with like 27 fields, so be sure to have all the names and contact info for your BAs easily reportable
- The audits will primarily be desk audits (on-line), although some on-site audits will be conducted
- There will be 200 audits, desk and on-site in 2016. Not sure if this number includes BAs
- Be sure to respond on time, maybe not too fast



MentorHealth

2016 Phase 2 OCR Audit Program…What We Do Know So Far

- Management refers to the appropriate privacy, security, and breach notification official(s) or person(s) designated by the covered entity or business associate for the implementation of policies and procedures and other standards;
- Unless otherwise specified, all document requests are for versions in use as of date of the audit notification and document request;
- Unless otherwise specified, selected entities should submit documents via OCR's secure online web portal in PDF, MS Word or MS Excel formats;
- If the requested number of documentations of implementation is not available, the entity must provide instances from previous years to complete the sample. If no documentation is available, the entity must provide a statement to that effect.

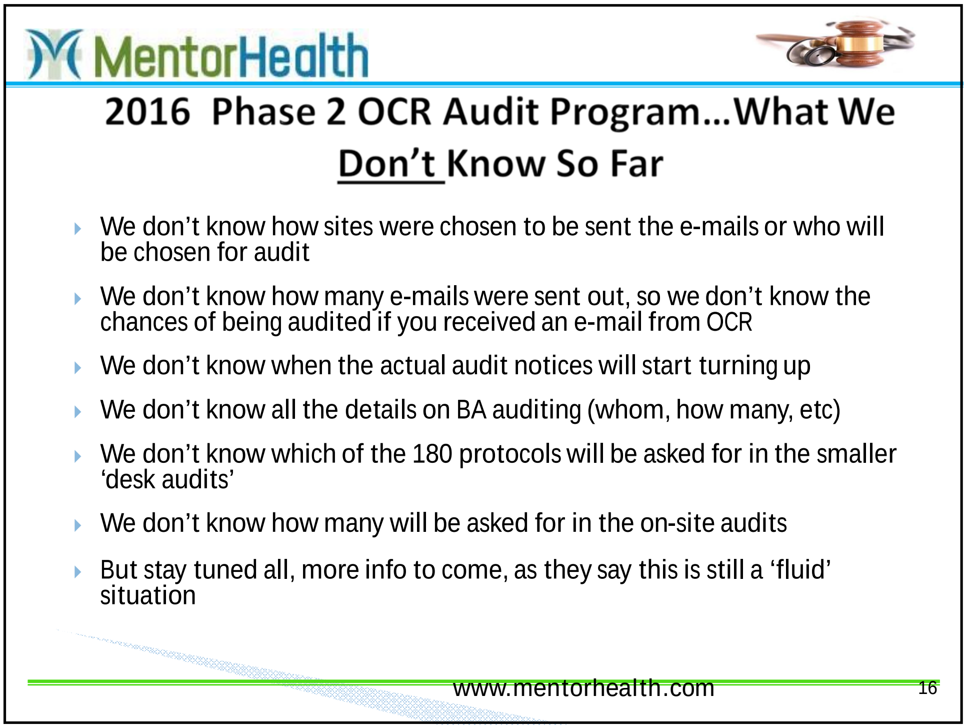


MentorHealth

Audit Program Link

- http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when

www.mentorhealth.com 15

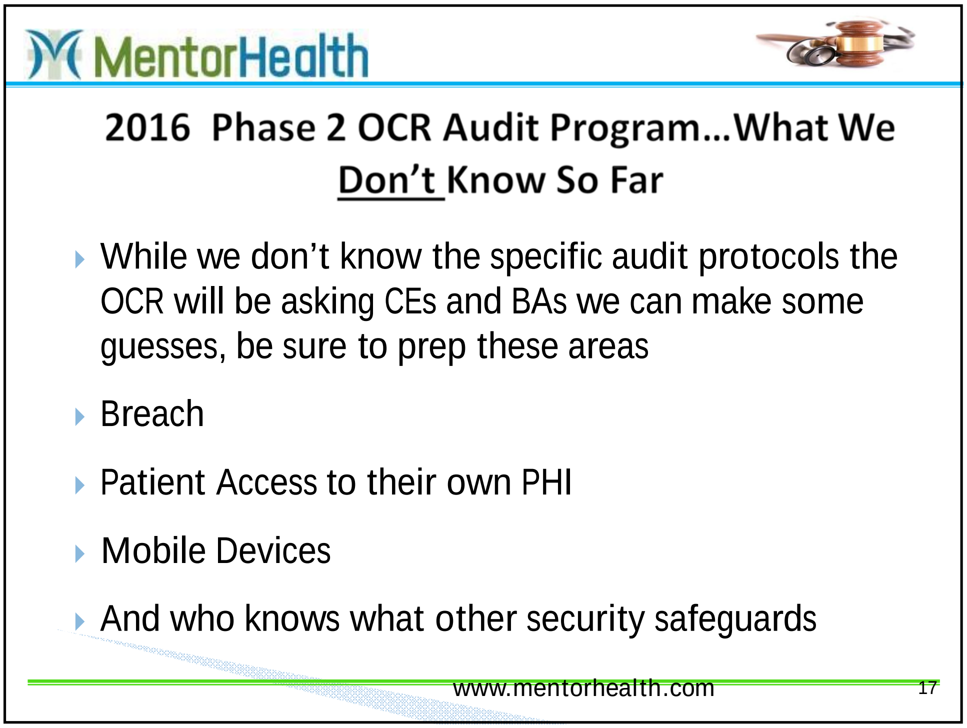


MentorHealth

2016 Phase 2 OCR Audit Program…What We Don't Know So Far

- We don't know how sites were chosen to be sent the e-mails or who will be chosen for audit
- We don't know how many e-mails were sent out, so we don't know the chances of being audited if you received an e-mail from OCR
- We don't know when the actual audit notices will start turning up
- We don't know all the details on BA auditing (whom, how many, etc)
- We don't know which of the 180 protocols will be asked for in the smaller 'desk audits'
- We don't know how many will be asked for in the on-site audits
- But stay tuned all, more info to come, as they say this is still a 'fluid' situation

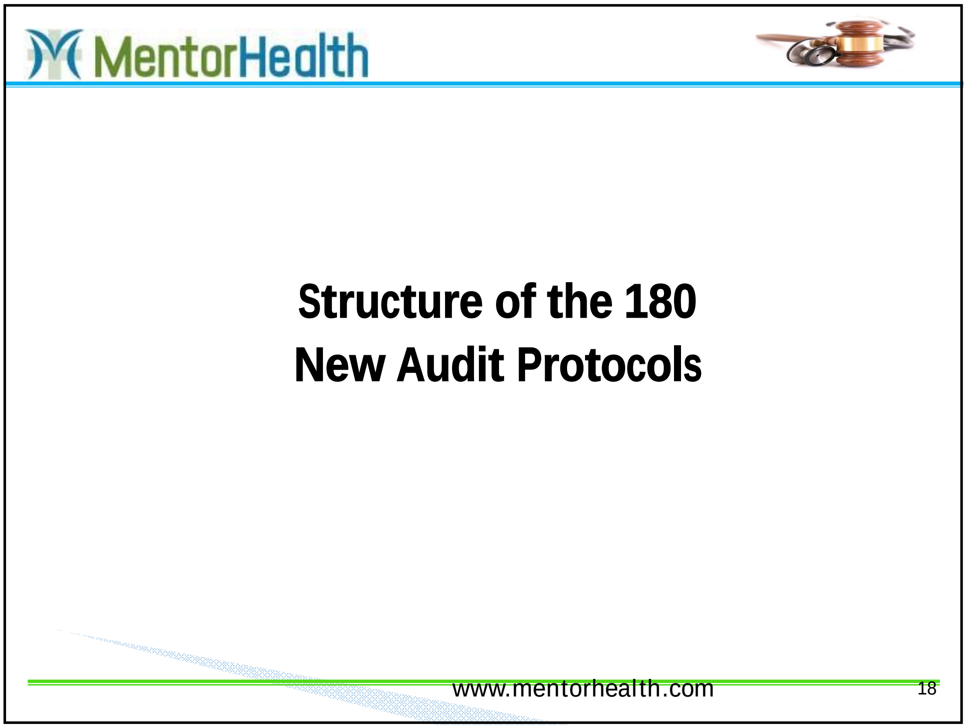
www.mentorhealth.com 16



2016 Phase 2 OCR Audit Program…What We Don't Know So Far

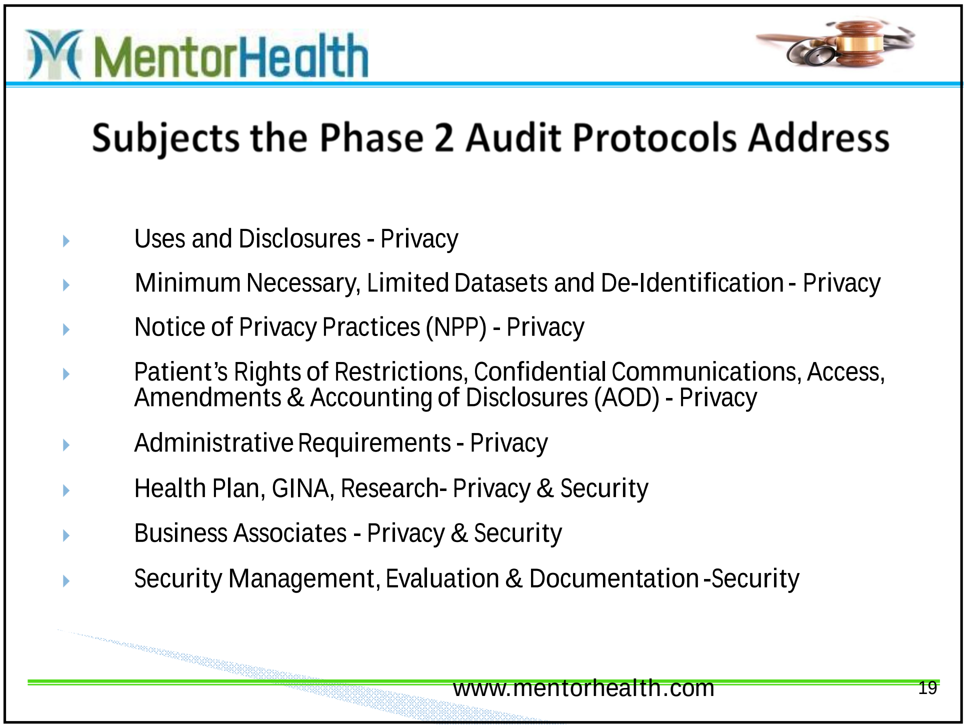
- While we don't know the specific audit protocols the OCR will be asking CEs and BAs we can make some guesses, be sure to prep these areas
- Breach
- Patient Access to their own PHI
- Mobile Devices
- And who knows what other security safeguards

www.mentorhealth.com 17



Structure of the 180 New Audit Protocols

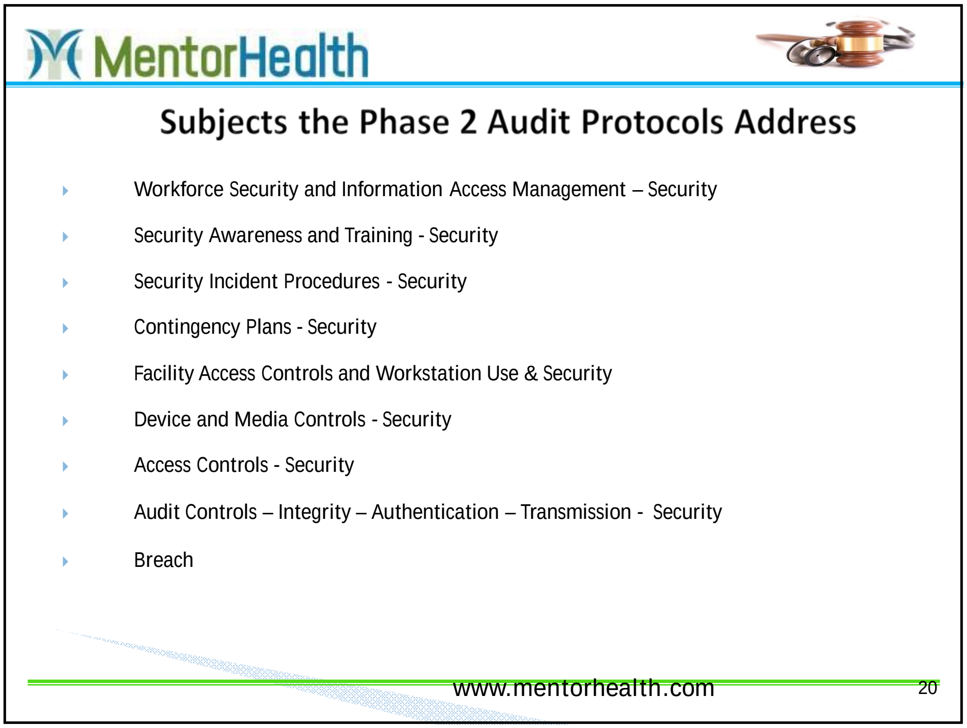
www.mentorhealth.com 18



MentorHealth

Subjects the Phase 2 Audit Protocols Address

- Uses and Disclosures - Privacy
- Minimum Necessary, Limited Datasets and De-Identification - Privacy
- Notice of Privacy Practices (NPP) - Privacy
- Patient’s Rights of Restrictions, Confidential Communications, Access, Amendments & Accounting of Disclosures (AOD) - Privacy
- Administrative Requirements - Privacy
- Health Plan, GINA, Research- Privacy & Security
- Business Associates - Privacy & Security
- Security Management, Evaluation & Documentation -Security



MentorHealth

Subjects the Phase 2 Audit Protocols Address

- Workforce Security and Information Access Management – Security
- Security Awareness and Training - Security
- Security Incident Procedures - Security
- Contingency Plans - Security
- Facility Access Controls and Workstation Use & Security
- Device and Media Controls - Security
- Access Controls - Security
- Audit Controls – Integrity – Authentication – Transmission - Security
- Breach

MentorHealth

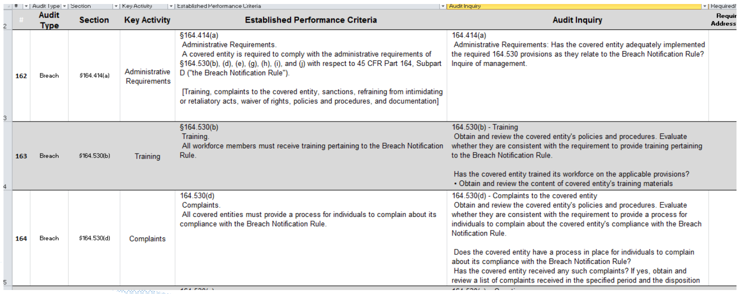
Number of 2016 Phase 2 Audit Protocols

- Privacy = 89
- Security = 72
- Breach = 19
- Total = 180 protocols
- Breach 19 protocols, 58 unique 'requests', 47 'requests using my consolidation
- Privacy 89 protocols, 172 unique requests, 128 using my consolidation

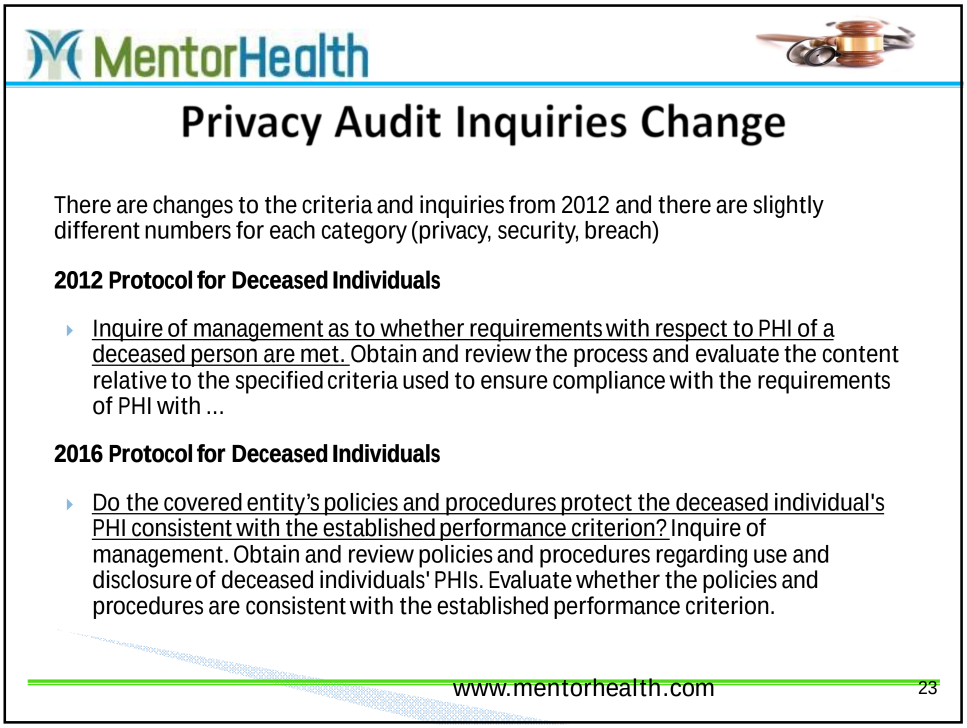
MentorHealth

Layout of the OCR Protocol Table

- Item Number
- Audit Type – Privacy, Security or Breach
- Section- Statute Number
- Key Activity – Important field of the major topic areas addressed
- Established Performance Criteria
- Audit Inquiry – Main statutory language and definitions if applicable
- Required/Addressable – For security protocols only, HIPAA security rule



#	Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	Requir Address
162	Breach	§164.414(a)	Administrative Requirements	§164.414(a) Administrative Requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule"). [Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and documentation]	164.414(a) Administrative Requirements: Has the covered entity adequately implemented the required 164.530 provisions as they relate to the Breach Notification Rule? Inquire of management.	
163	Breach	§164.530(b)	Training	§164.530(b) Training. All workforce members must receive training pertaining to the Breach Notification Rule.	164.530(b) - Training Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to provide training pertaining to the Breach Notification Rule. Has the covered entity trained its workforce on the applicable provisions? • Obtain and review the content of covered entity's training materials	
164	Breach	§164.530(d)	Complaints	164.530(d) Complaints. All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.	164.530(d) - Complaints to the covered entity Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent with the requirement to provide a process for individuals to complain about the covered entity's compliance with the Breach Notification Rule. Does the covered entity have a process in place for individuals to complain about its compliance with the Breach Notification Rule? Has the covered entity received any such complaints? If yes, obtain and review a list of complaints received in the specified period and the disposition	



MentorHealth

Privacy Audit Inquiries Change

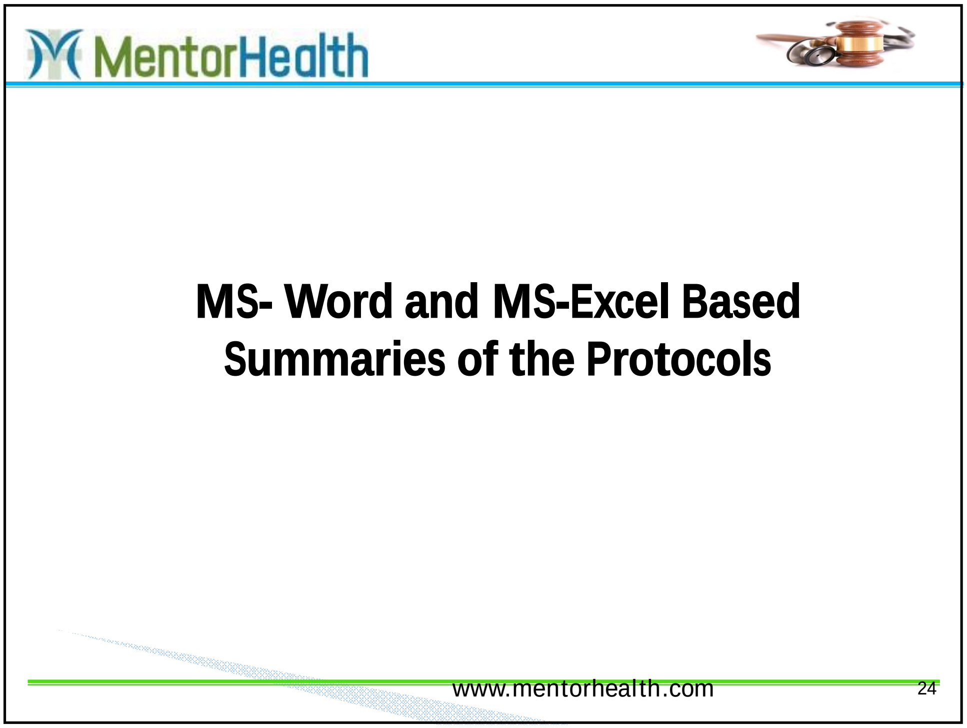
There are changes to the criteria and inquiries from 2012 and there are slightly different numbers for each category (privacy, security, breach)

2012 Protocol for 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 …

2016 Protocol for Deceased Individuals

- Do the covered entity's policies and procedures protect the deceased individual's PHI consistent with the established performance criterion? Inquire of management. Obtain and review policies and procedures regarding use and disclosure of deceased individuals' PHIs. Evaluate whether the policies and procedures are consistent with the established performance criterion.



MentorHealth

MS- Word and MS-Excel Based Summaries of the Protocols

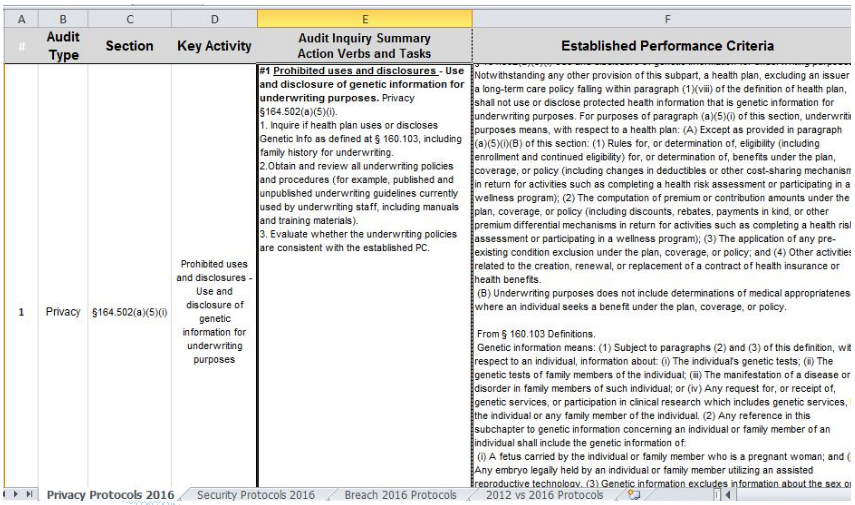
MentorHealth

OCR Audit Protocol Summaries By Kelly McLendon

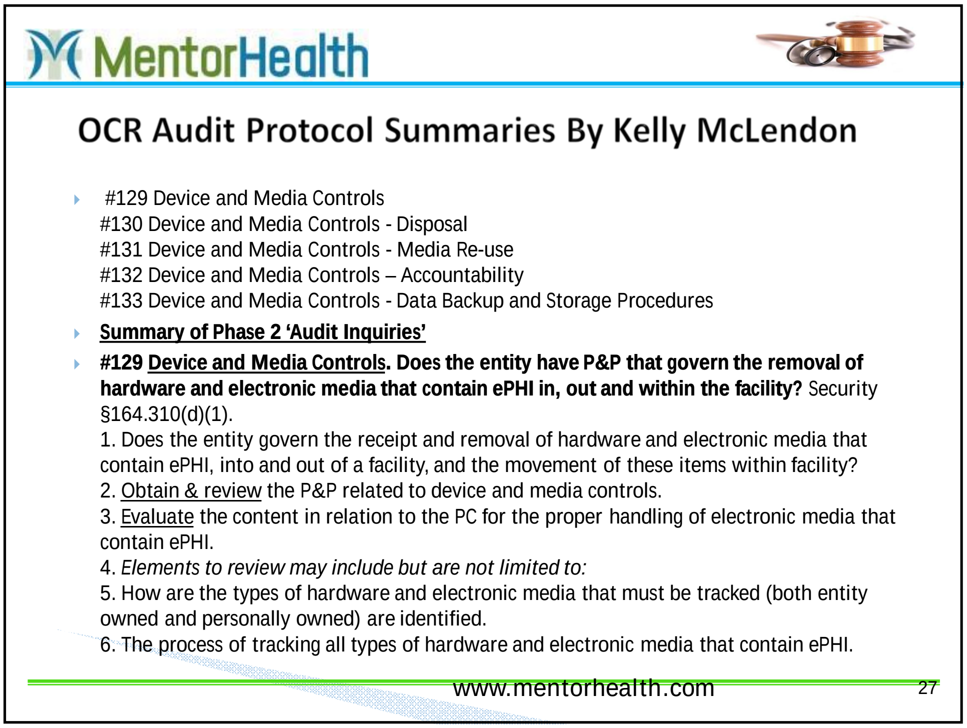
- I created a new summary column in an MS-Excel document copied from the OCR audit protocol tables
- Then converted the column into a MS-Word document in order to more easily work with the protocols (since there are so many of them!)
- We will either provide copies of these documents to you for download or you can request directly from Kelly at kmclendon@complianceprosolutions.com

MentorHealth

OCR Audit Protocol Summaries By Kelly McLendon



A	B	C	D	E	F
#	Audit Type	Section	Key Activity	Audit Inquiry Summary Action Verbs and Tasks	Established Performance Criteria
1	Privacy	§164.502(a)(5)(i)	Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes	**#1 <u>Prohibited uses and disclosures</u> - Use and disclosure of genetic information for underwriting purposes.** Privacy §164.502(a)(5)(i). 1. Inquire if health plan uses or discloses Genetic Info as defined at § 160.103, including family history for underwriting. 2.Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials). 3. Evaluate whether the underwriting policies are consistent with the established PC.	Notwithstanding any other provision of this subpart, a health plan, excluding an issuer a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriti purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanism in return for activities such as completing a health risk assessment or participating in a wellness program); (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risl assessment or participating in a wellness program); (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. (B) Underwriting purposes does not include determinations of medical appropriatenes where an individual seeks a benefit under the plan, coverage, or policy. From § 160.103 Definitions. Genetic information means: (1) Subject to paragraphs (2) and (3) of this definition, wit respect to an individual, information about: (i) The individual's genetic tests; (ii) The genetic tests of family members of the individual; (iii) The manifestation of a disease or disorder in family members of such individual; or (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, the individual or any family member of the individual. (2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of: (i) A fetus carried by the individual or family member who is a pregnant woman; and (Any embryo legally held by an individual or family member utilizing an assisted reproductive technology. (3) Genetic information excludes information about the sex o

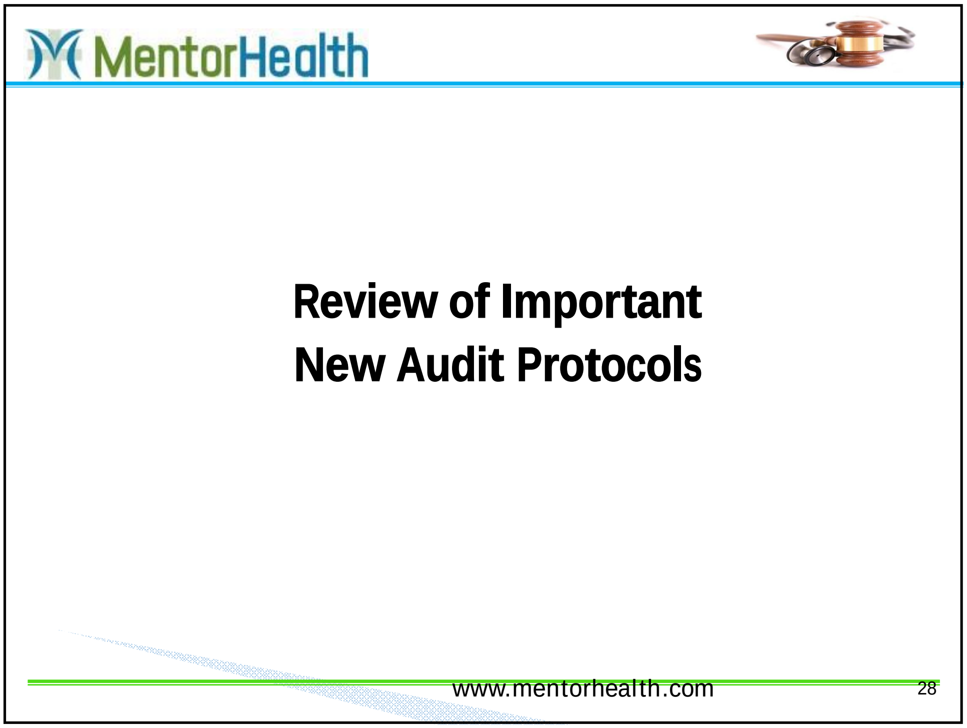


MentorHealth

OCR Audit Protocol Summaries By Kelly McLendon

- #129 Device and Media Controls
  #130 Device and Media Controls - Disposal
  #131 Device and Media Controls - Media Re-use
  #132 Device and Media Controls – Accountability
  #133 Device and Media Controls - Data Backup and Storage Procedures
- **<u>Summary of Phase 2 ‘Audit Inquiries’</u>**
- **#129 <u>Device and Media Controls</u>. Does the entity have P&P that govern the removal of hardware and electronic media that contain ePHI in, out and within the facility?** Security §164.310(d)(1).
  1. Does the entity 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 facility?
  2. <u>Obtain & review</u> the P&P related to device and media controls.
  3. <u>Evaluate</u> the content in relation to the PC for the proper handling of electronic media that contain ePHI.
  4. *Elements to review may include but are not limited to:*
  5. How are the types of hardware and electronic media that must be tracked (both entity owned and personally owned) are identified.
  6. The process of tracking all types of hardware and electronic media that contain ePHI.

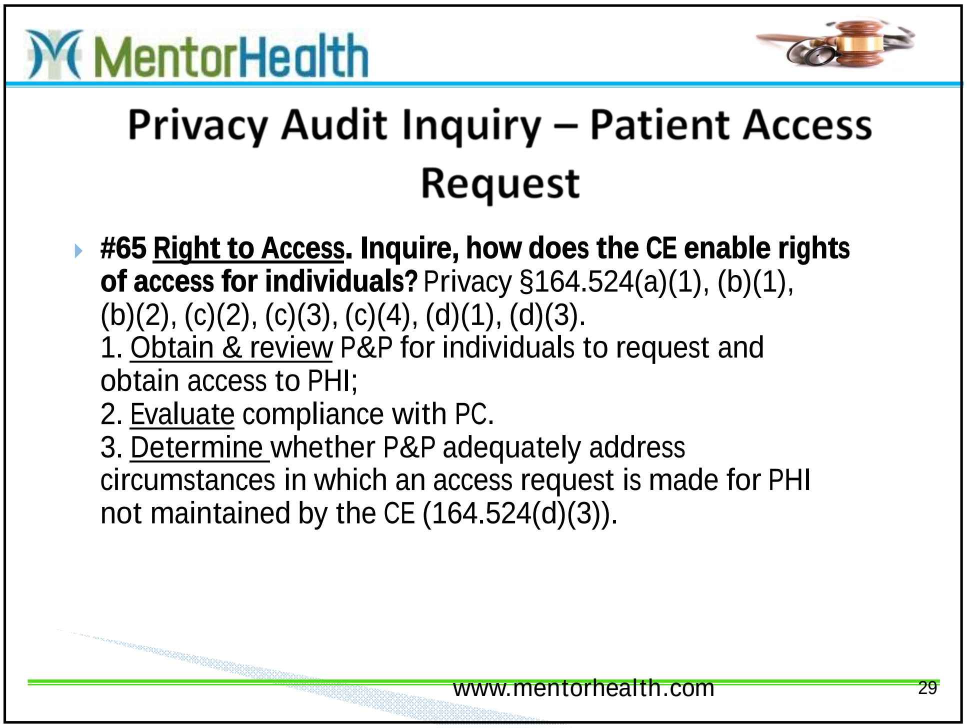
www.mentorhealth.com 27



MentorHealth

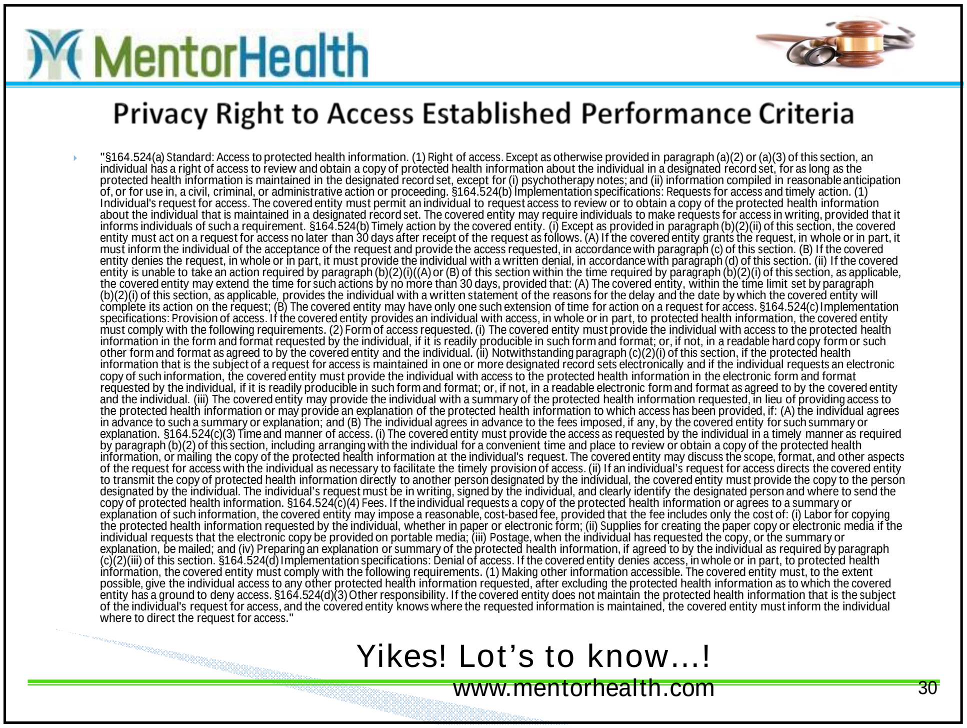
Review of Important New Audit Protocols

www.mentorhealth.com 28



Privacy Audit Inquiry – Patient Access Request

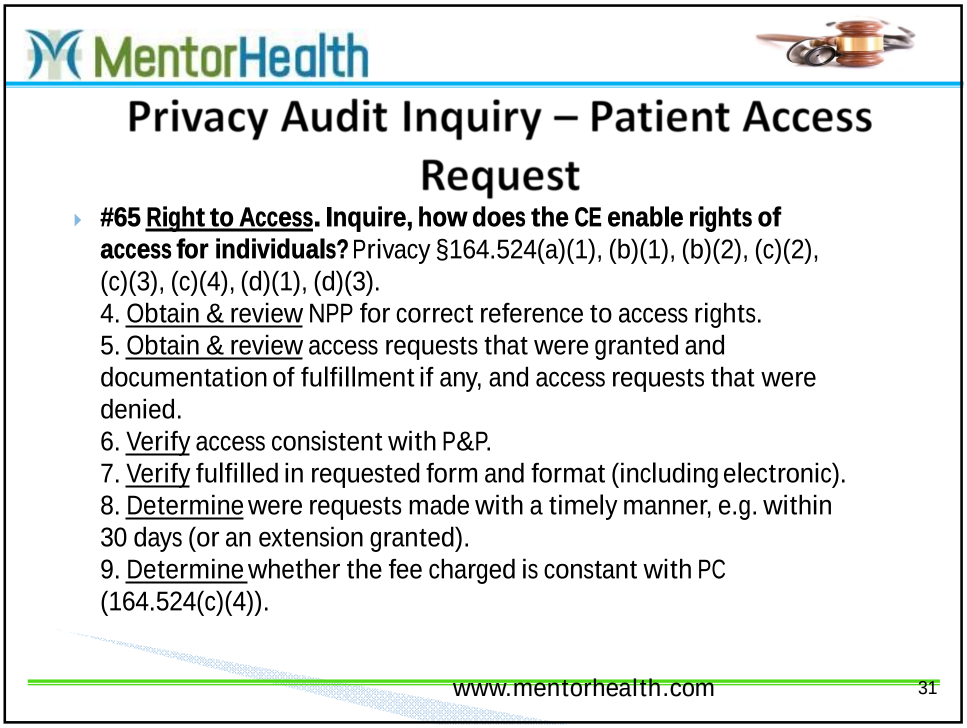
- **#65 <u>Right to Access</u>. Inquire, how does the CE enable rights of access for individuals?** Privacy §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3).
  1. <u>Obtain & review</u> P&P for individuals to request and obtain access to PHI;
  2. <u>Evaluate</u> compliance with PC.
  3. <u>Determine</u> whether P&P adequately address circumstances in which an access request is made for PHI not maintained by the CE (164.524(d)(3)).



Privacy Right to Access Established Performance Criteria

- "§164.524(a) Standard: Access to protected health information. (1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to review and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for (i) psychotherapy notes; and (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. §164.524(b) Implementation specifications: Requests for access and timely action. (1) Individual's request for access. The covered entity must permit an individual to request access to review or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement. §164.524(b) Timely action by the covered entity. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows. (A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section. (B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section. (ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)((A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that: (A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; (B) The covered entity may have only one such extension of time for action on a request for access. §164.524(c) Implementation specifications: Provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements. (2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. (ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. (iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if: (A) the individual agrees in advance to such a summary or explanation; and (B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation. §164.524(c)(3) Time and manner of access. (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to review or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access. (ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information. §164.524(c)(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of: (i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form; (ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; (iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and (iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section. §164.524(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements. (1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access. §164.524(d)(3) Other responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access."

Yikes! Lot's to know…!

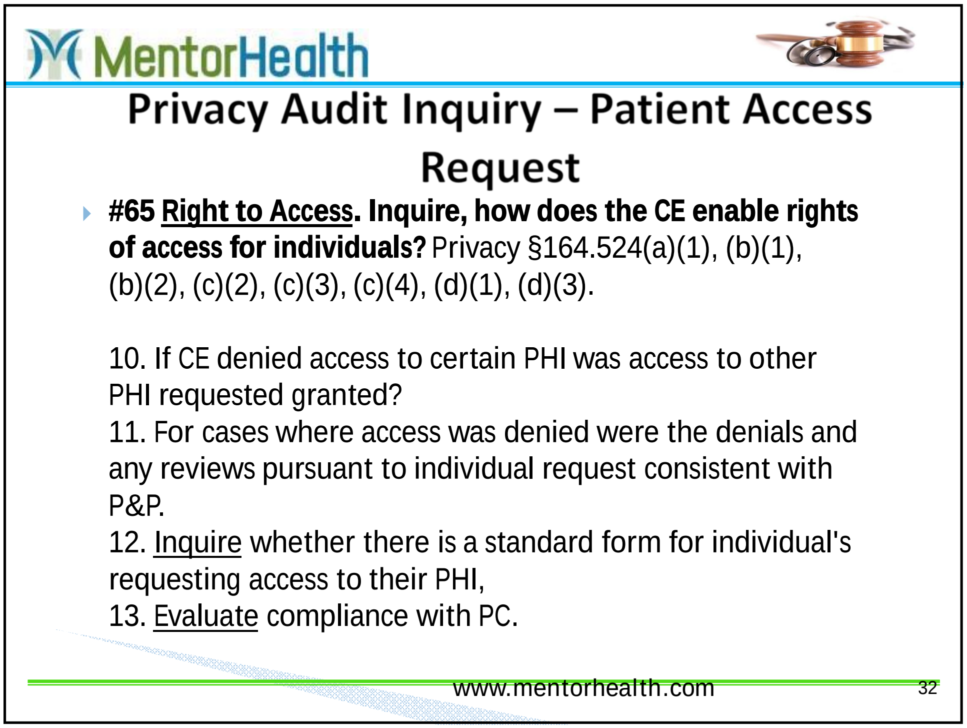


MentorHealth

Privacy Audit Inquiry – Patient Access Request

- **#65 Right to Access. Inquire, how does the CE enable rights of access for individuals?** Privacy §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3).
  4. Obtain & review NPP for correct reference to access rights.
  5. Obtain & review access requests that were granted and documentation of fulfillment if any, and access requests that were denied.
  6. Verify access consistent with P&P.
  7. Verify fulfilled in requested form and format (including electronic).
  8. Determine were requests made with a timely manner, e.g. within 30 days (or an extension granted).
  9. Determine whether the fee charged is constant with PC (164.524(c)(4)).

www.mentorhealth.com 31



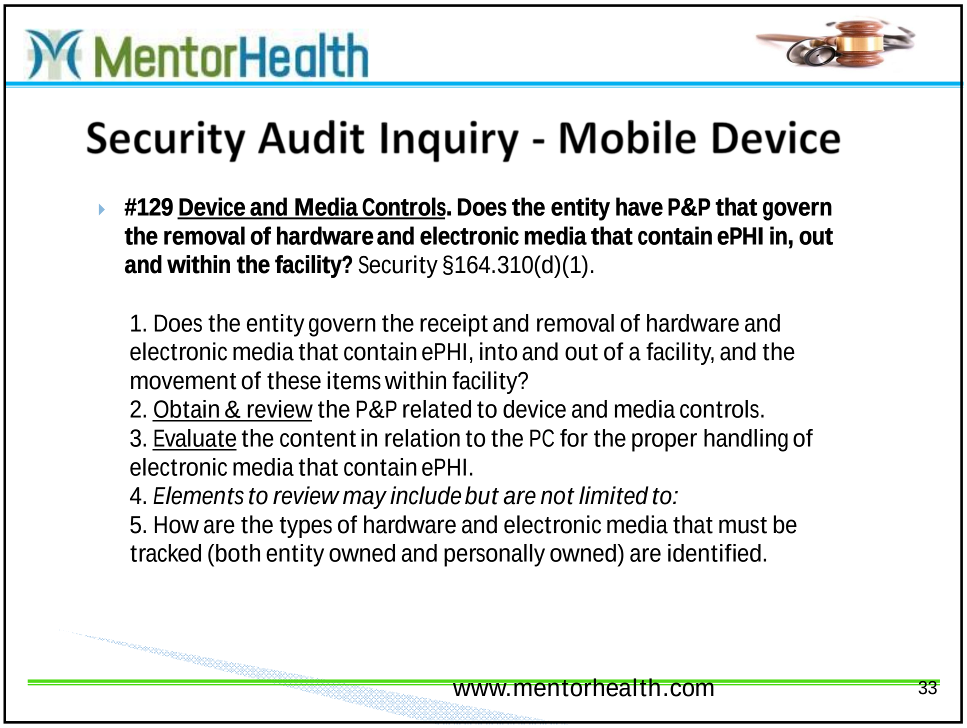
MentorHealth

Privacy Audit Inquiry – Patient Access Request

- **#65 Right to Access. Inquire, how does the CE enable rights of access for individuals?** Privacy §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3).

  10. If CE denied access to certain PHI was access to other PHI requested granted?
  11. For cases where access was denied were the denials and any reviews pursuant to individual request consistent with P&P.
  12. Inquire whether there is a standard form for individual's requesting access to their PHI,
  13. Evaluate compliance with PC.

www.mentorhealth.com 32



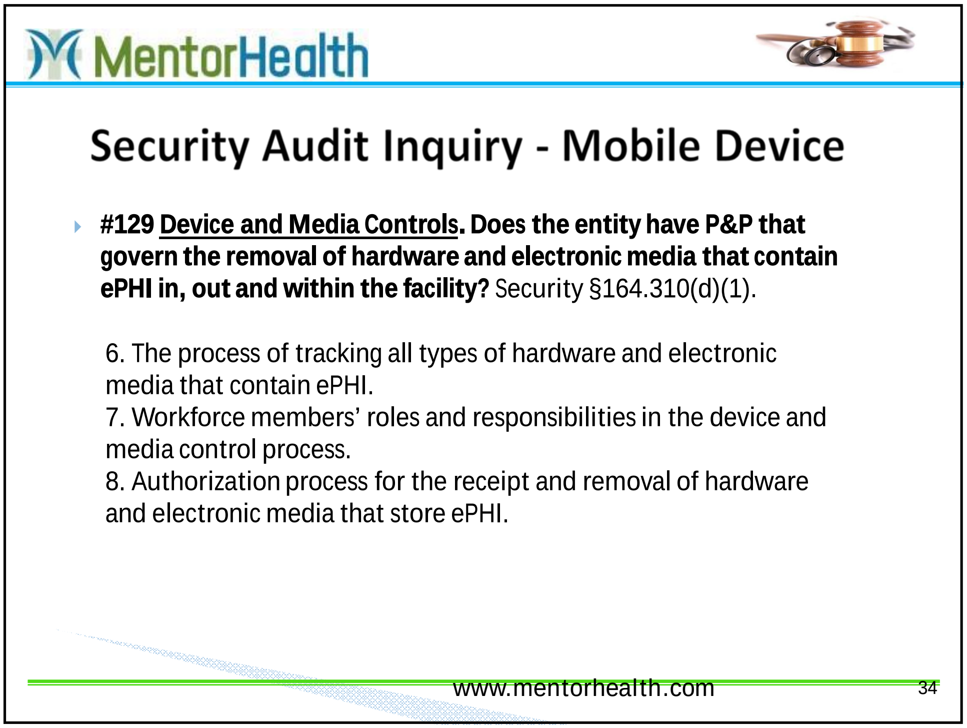
MentorHealth

Security Audit Inquiry - Mobile Device

- **#129 <u>Device and Media Controls</u>. Does the entity have P&P that govern the removal of hardware and electronic media that contain ePHI in, out and within the facility?** Security §164.310(d)(1).

1. Does the entity 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 facility?
2. <u>Obtain & review</u> the P&P related to device and media controls.
3. <u>Evaluate</u> the content in relation to the PC for the proper handling of electronic media that contain ePHI.
4. *Elements to review may include but are not limited to:*
5. How are the types of hardware and electronic media that must be tracked (both entity owned and personally owned) are identified.

www.mentorhealth.com 33



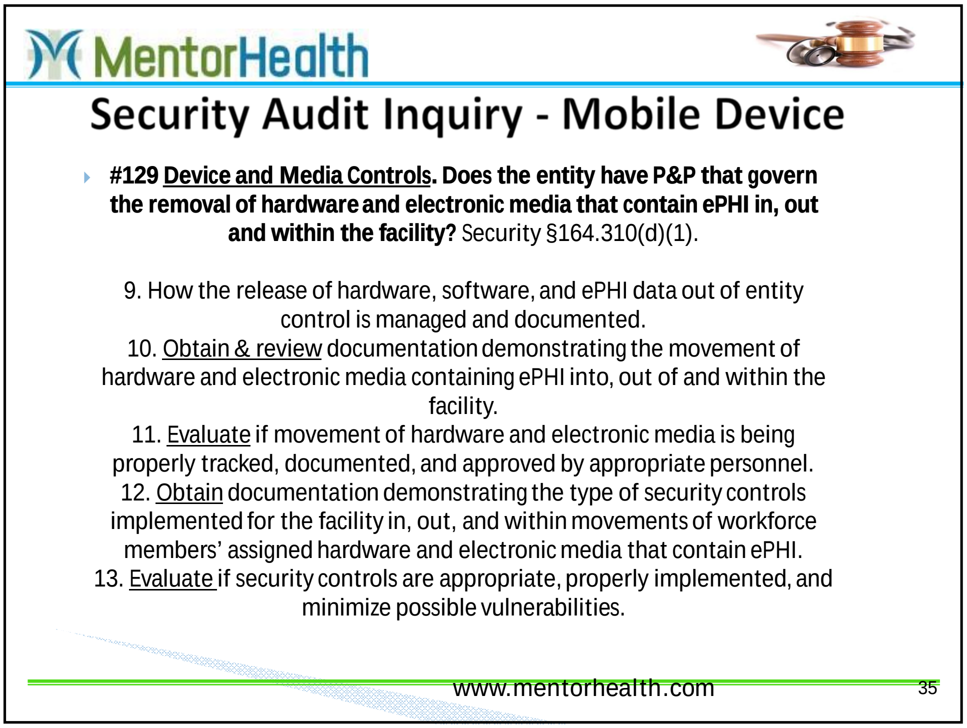
MentorHealth

Security Audit Inquiry - Mobile Device

- **#129 <u>Device and Media Controls</u>. Does the entity have P&P that govern the removal of hardware and electronic media that contain ePHI in, out and within the facility?** Security §164.310(d)(1).

6. The process of tracking all types of hardware and electronic media that contain ePHI.
7. Workforce members’ roles and responsibilities in the device and media control process.
8. Authorization process for the receipt and removal of hardware and electronic media that store ePHI.

www.mentorhealth.com 34

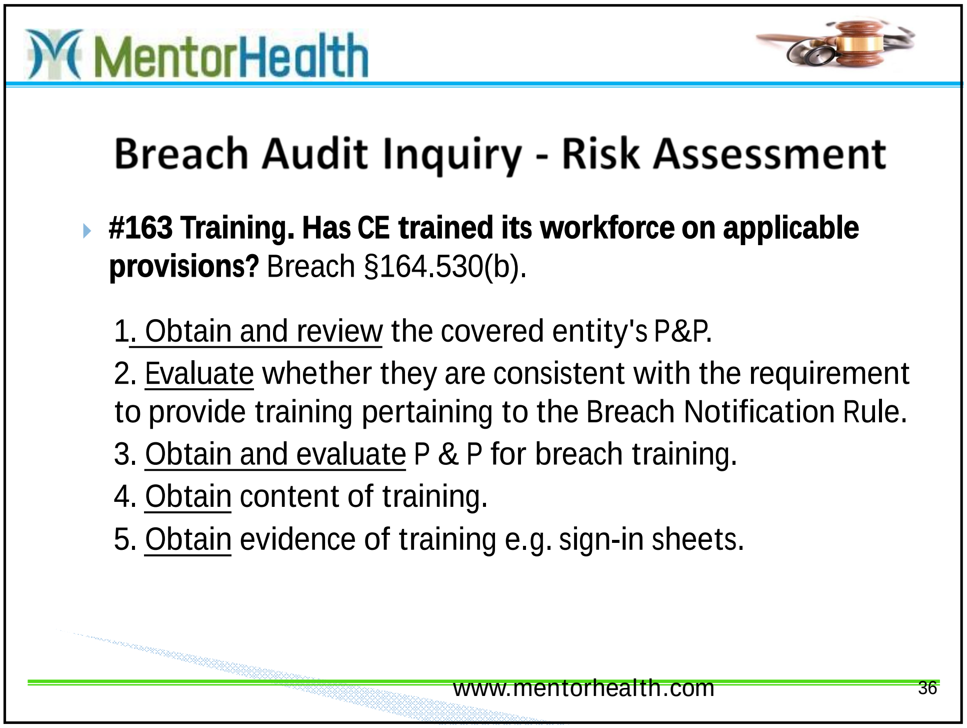


MentorHealth

Security Audit Inquiry - Mobile Device

- **#129 Device and Media Controls. Does the entity have P&P that govern the removal of hardware and electronic media that contain ePHI in, out and within the facility?** Security §164.310(d)(1).

9. How the release of hardware, software, and ePHI data out of entity control is managed and documented.
10. Obtain & review documentation demonstrating the movement of hardware and electronic media containing ePHI into, out of and within the facility.
11. Evaluate if movement of hardware and electronic media is being properly tracked, documented, and approved by appropriate personnel.
12. Obtain documentation demonstrating the type of security controls implemented for the facility in, out, and within movements of workforce members' assigned hardware and electronic media that contain ePHI.
13. Evaluate if security controls are appropriate, properly implemented, and minimize possible vulnerabilities.

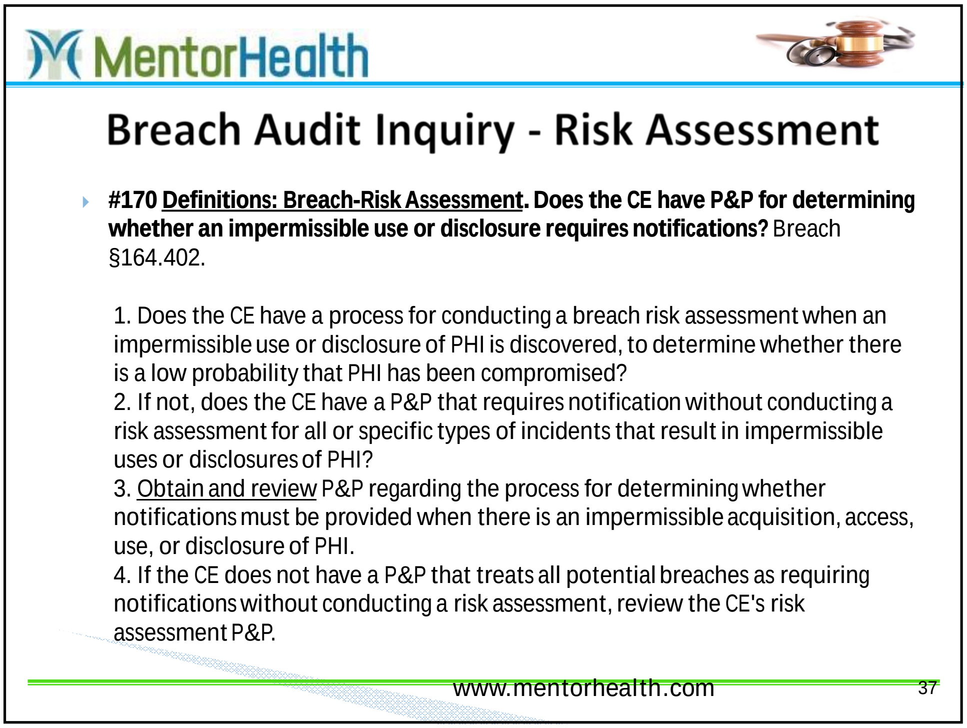


MentorHealth

Breach Audit Inquiry - Risk Assessment

- **#163 Training. Has CE trained its workforce on applicable provisions?** Breach §164.530(b).

1. Obtain and review the covered entity's P&P.
2. Evaluate whether they are consistent with the requirement to provide training pertaining to the Breach Notification Rule.
3. Obtain and evaluate P & P for breach training.
4. Obtain content of training.
5. Obtain evidence of training e.g. sign-in sheets.



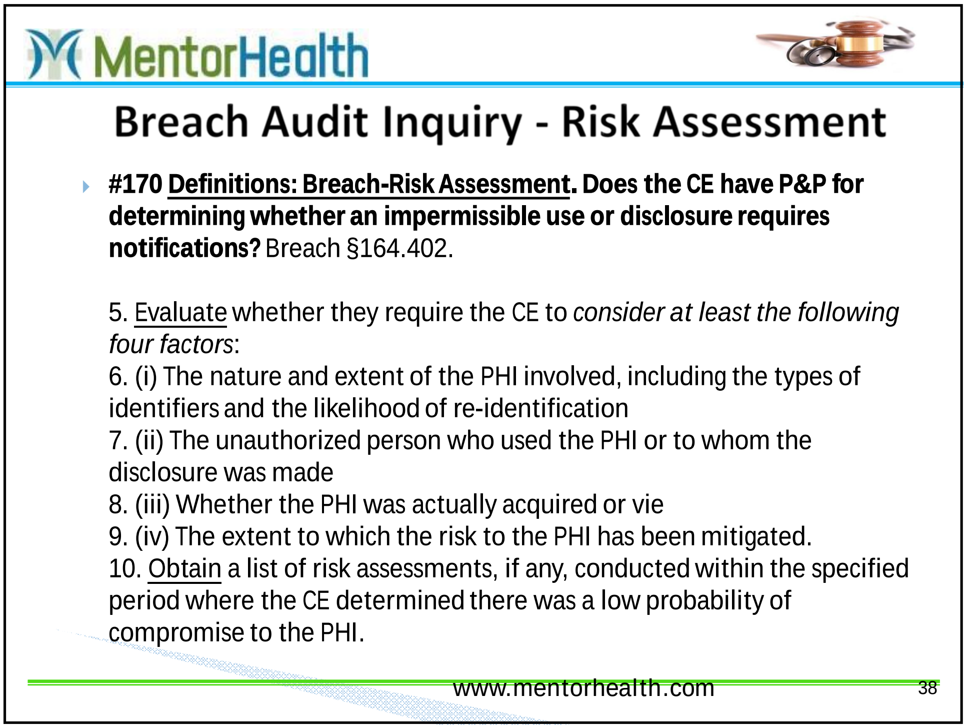
MentorHealth

Breach Audit Inquiry - Risk Assessment

- **#170 Definitions: Breach-Risk Assessment. Does the CE have P&P for determining whether an impermissible use or disclosure requires notifications?** Breach §164.402.

  1. Does the CE have a process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised?
  2. If not, does the CE have a P&P that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI?
  3. Obtain and review P&P regarding the process for determining whether notifications must be provided when there is an impermissible acquisition, access, use, or disclosure of PHI.
  4. If the CE does not have a P&P that treats all potential breaches as requiring notifications without conducting a risk assessment, review the CE's risk assessment P&P.

www.mentorhealth.com 37



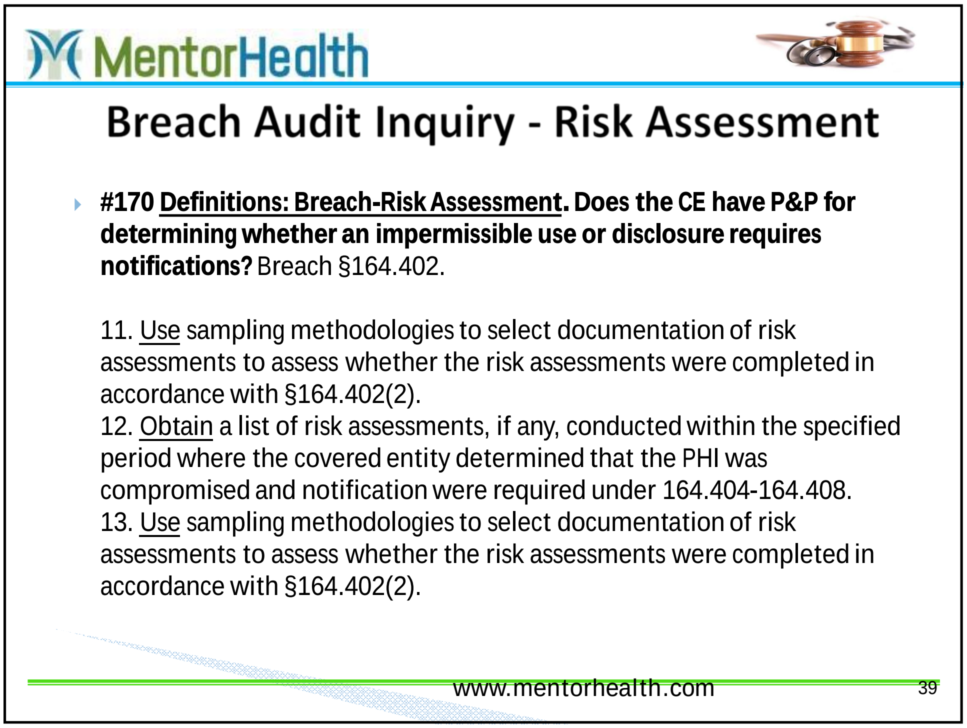
MentorHealth

Breach Audit Inquiry - Risk Assessment

- **#170 Definitions: Breach-Risk Assessment. Does the CE have P&P for determining whether an impermissible use or disclosure requires notifications?** Breach §164.402.

  5. Evaluate whether they require the CE to *consider at least the following four factors*:
  6. (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  7. (ii) The unauthorized person who used the PHI or to whom the disclosure was made
  8. (iii) Whether the PHI was actually acquired or vie
  9. (iv) The extent to which the risk to the PHI has been mitigated.
  10. Obtain a list of risk assessments, if any, conducted within the specified period where the CE determined there was a low probability of compromise to the PHI.

www.mentorhealth.com 38

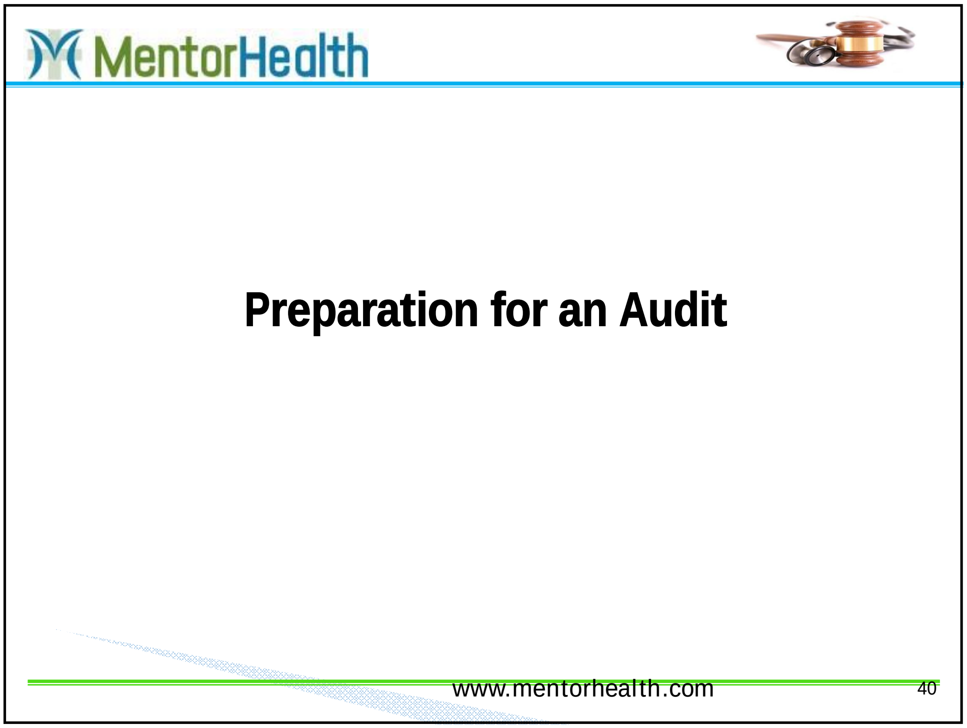


MentorHealth

Breach Audit Inquiry - Risk Assessment

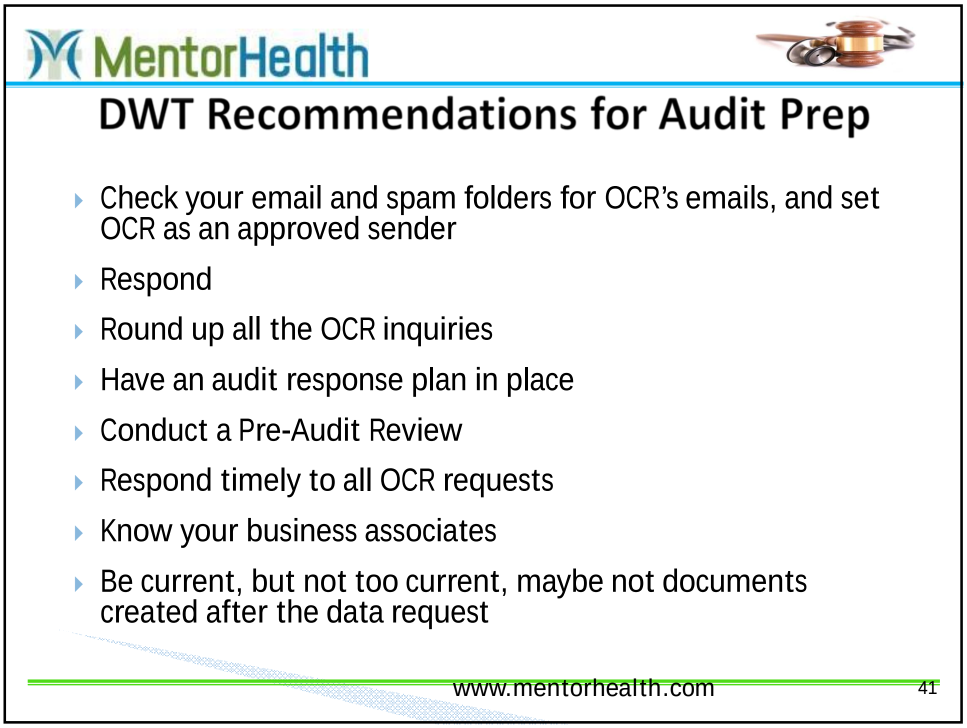
- **#170 <u>Definitions: Breach-Risk Assessment</u>. Does the CE have P&P for determining whether an impermissible use or disclosure requires notifications?** Breach §164.402.

  11. <u>Use</u> sampling methodologies to select documentation of risk assessments to assess whether the risk assessments were completed in accordance with §164.402(2).
  12. <u>Obtain</u> a list of risk assessments, if any, conducted within the specified period where the covered entity determined that the PHI was compromised and notification were required under 164.404-164.408.
  13. <u>Use</u> sampling methodologies to select documentation of risk assessments to assess whether the risk assessments were completed in accordance with §164.402(2).



MentorHealth

Preparation for an Audit

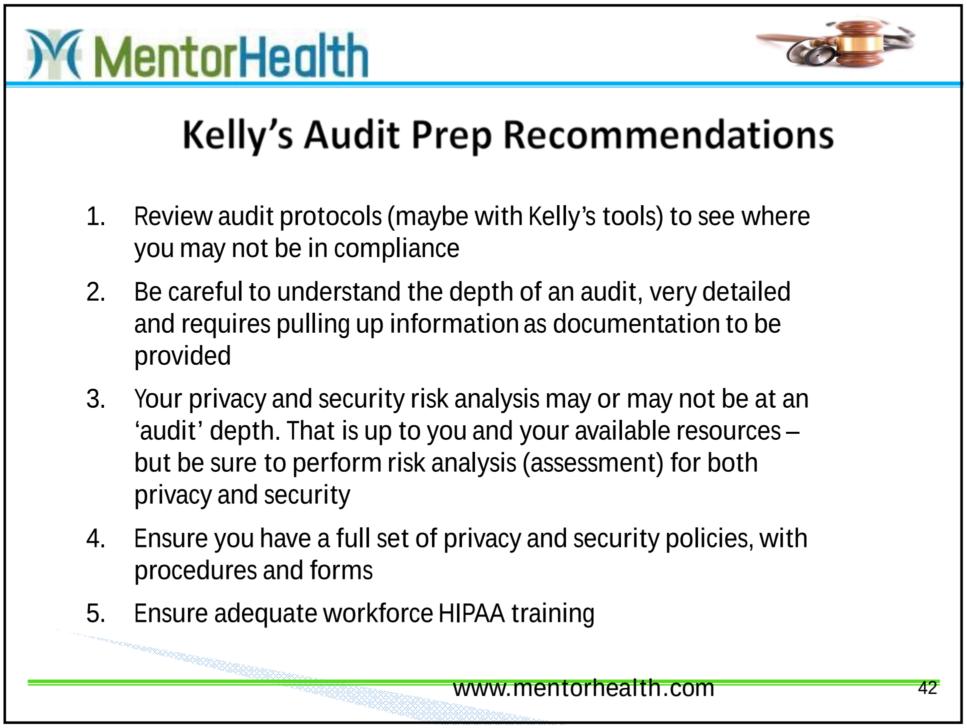


MentorHealth

DWT Recommendations for Audit Prep

- Check your email and spam folders for OCR's emails, and set OCR as an approved sender
- Respond
- Round up all the OCR inquiries
- Have an audit response plan in place
- Conduct a Pre-Audit Review
- Respond timely to all OCR requests
- Know your business associates
- Be current, but not too current, maybe not documents created after the data request

www.mentorhealth.com 41

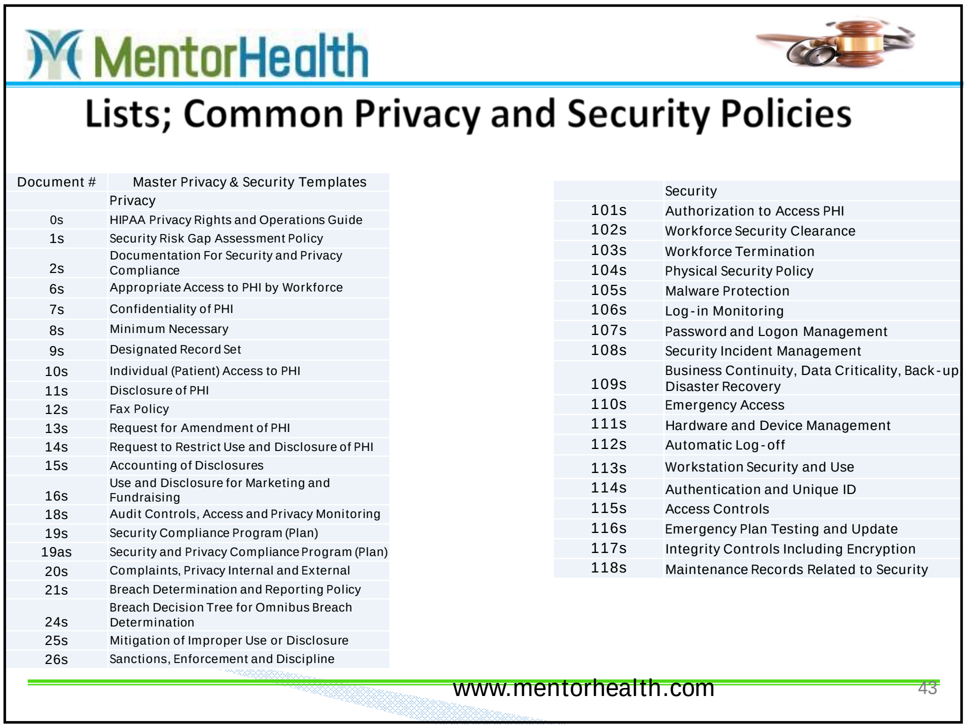


MentorHealth

Kelly's Audit Prep Recommendations

1. Review audit protocols (maybe with Kelly's tools) to see where you may not be in compliance
2. Be careful to understand the depth of an audit, very detailed and requires pulling up information as documentation to be provided
3. Your privacy and security risk analysis may or may not be at an 'audit' depth. That is up to you and your available resources – but be sure to perform risk analysis (assessment) for both privacy and security
4. Ensure you have a full set of privacy and security policies, with procedures and forms
5. Ensure adequate workforce HIPAA training

www.mentorhealth.com 42



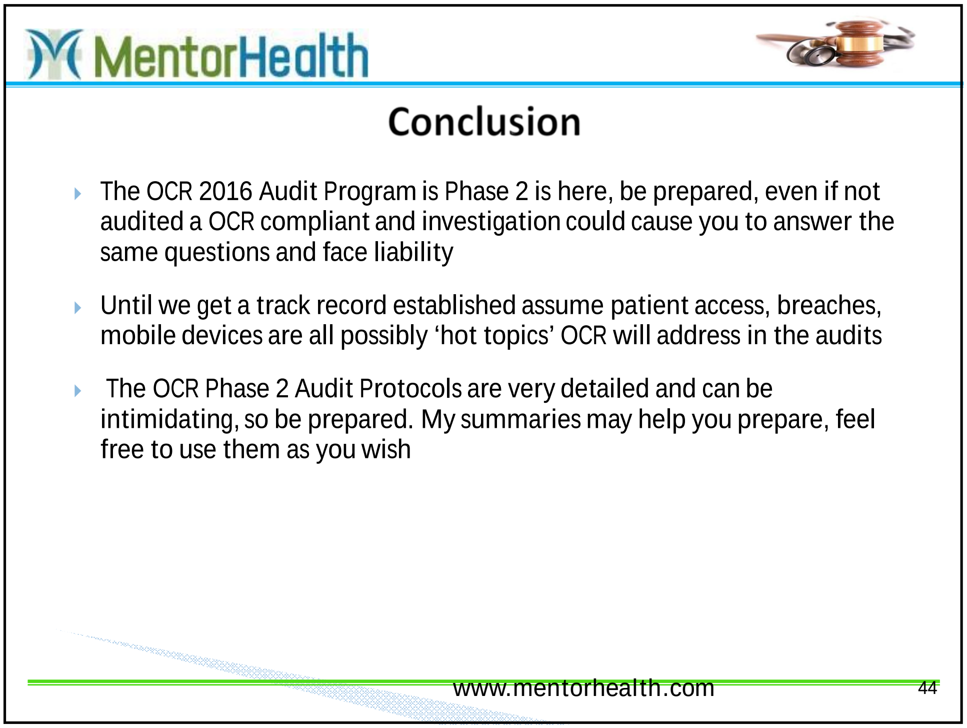
MentorHealth

Lists; Common Privacy and Security Policies

Document #	Master Privacy & Security Templates
	Privacy
0s	HIPAA Privacy Rights and Operations Guide
1s	Security Risk Gap Assessment Policy
2s	Documentation For Security and Privacy Compliance
6s	Appropriate Access to PHI by Workforce
7s	Confidentiality of PHI
8s	Minimum Necessary
9s	Designated Record Set
10s	Individual (Patient) Access to PHI
11s	Disclosure of PHI
12s	Fax Policy
13s	Request for Amendment of PHI
14s	Request to Restrict Use and Disclosure of PHI
15s	Accounting of Disclosures
16s	Use and Disclosure for Marketing and Fundraising
18s	Audit Controls, Access and Privacy Monitoring
19s	Security Compliance Program (Plan)
19as	Security and Privacy Compliance Program (Plan)
20s	Complaints, Privacy Internal and External
21s	Breach Determination and Reporting Policy
24s	Breach Decision Tree for Omnibus Breach Determination
25s	Mitigation of Improper Use or Disclosure
26s	Sanctions, Enforcement and Discipline

	Security
101s	Authorization to Access PHI
102s	Workforce Security Clearance
103s	Workforce Termination
104s	Physical Security Policy
105s	Malware Protection
106s	Log-in Monitoring
107s	Password and Logon Management
108s	Security Incident Management
109s	Business Continuity, Data Criticality, Back-up Disaster Recovery
110s	Emergency Access
111s	Hardware and Device Management
112s	Automatic Log-off
113s	Workstation Security and Use
114s	Authentication and Unique ID
115s	Access Controls
116s	Emergency Plan Testing and Update
117s	Integrity Controls Including Encryption
118s	Maintenance Records Related to Security

www.mentorhealth.com 43

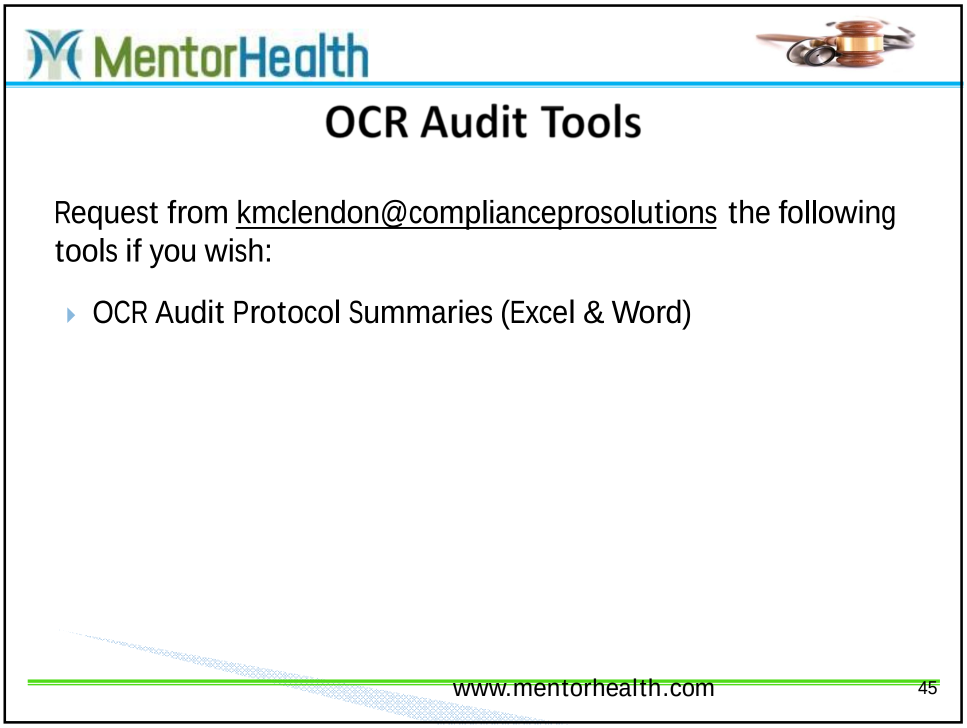


MentorHealth

Conclusion

- The OCR 2016 Audit Program is Phase 2 is here, be prepared, even if not audited a OCR compliant and investigation could cause you to answer the same questions and face liability
- Until we get a track record established assume patient access, breaches, mobile devices are all possibly ‘hot topics’ OCR will address in the audits
- The OCR Phase 2 Audit Protocols are very detailed and can be intimidating, so be prepared. My summaries may help you prepare, feel free to use them as you wish

www.mentorhealth.com 44

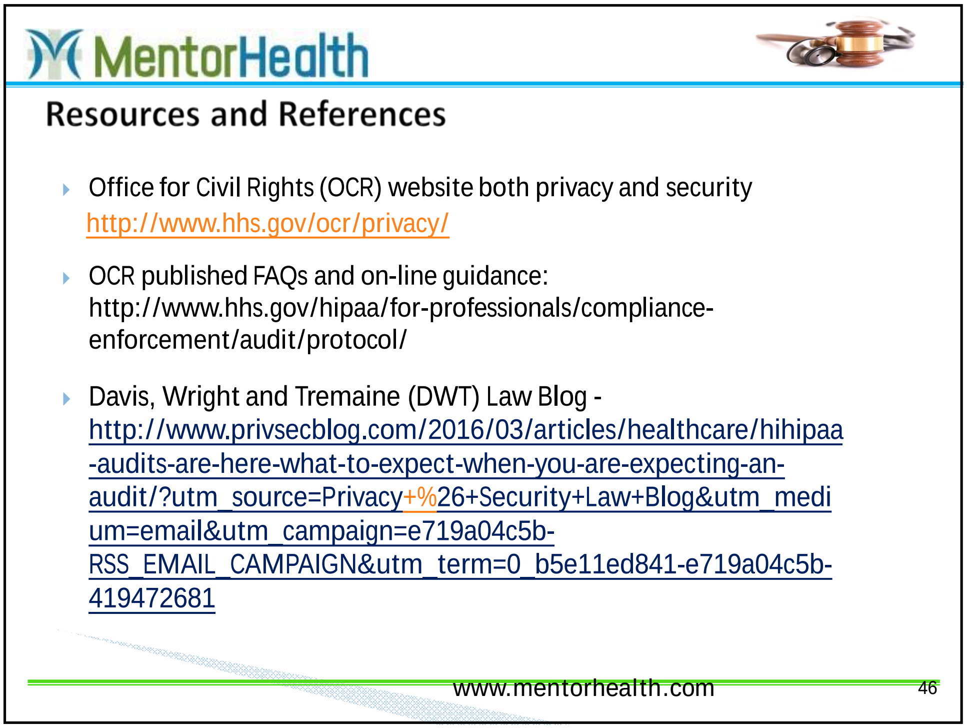


MentorHealth

OCR Audit Tools

Request from kmclendon@complianceprosolutions the following tools if you wish:

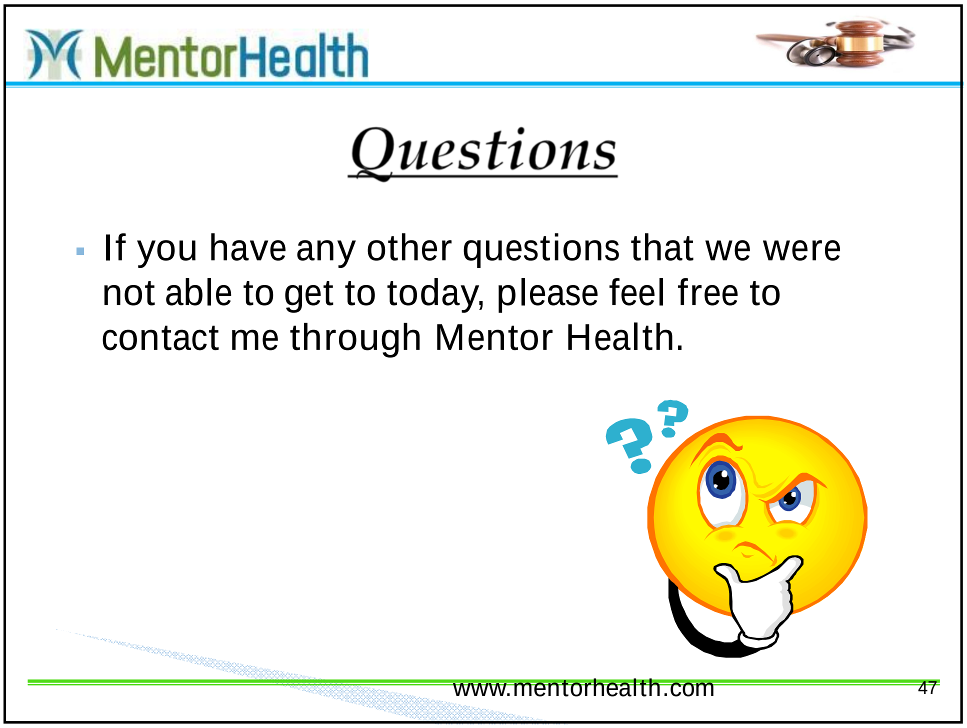
- OCR Audit Protocol Summaries (Excel & Word)



MentorHealth

Resources and References

- Office for Civil Rights (OCR) website both privacy and security http://www.hhs.gov/ocr/privacy/
- OCR published FAQs and on-line guidance: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/
- Davis, Wright and Tremaine (DWT) Law Blog - http://www.privsecblog.com/2016/03/articles/healthcare/hihipaa-audits-are-here-what-to-expect-when-you-are-expecting-an-audit/?utm_source=Privacy+%26+Security+Law+Blog&utm_medium=email&utm_campaign=e719a04c5b-RSS_EMAIL_CAMPAIGN&utm_term=0_b5e11ed841-e719a04c5b-419472681



MentorHealth

Questions

- If you have any other questions that we were not able to get to today, please feel free to contact me through Mentor Health.

MentorHealth

Contact Us:

- ***Customer Support at :***
  1.800.385.1607
- ***Questions/comments/suggestions:***
  webinars@mentorhealth.com
- ***Partners & Resellers:***
  partner@mentorhealth.com