HIPAA Audits Are Here!

How to prepare for and what to expect when OCR comes knocking – May 12, 2016

James B. Wieland, Principal, Ober|Kaler
Emily H. Wein, Principal, Ober|Kaler
David Holtzman, VP of Compliance, CynergisTek

OBER | KALER
Attorneys at Law

CYNERGISTEK

Background

- HITECH (2009) required HHS Office for Civil Rights (OCR) to conduct periodic audits of covered entities and business associates
  - Audits are to focus on compliance with Privacy, Security and Breach Notification Rules
- Pilot audit program in 2011 and 2012
  - Assessed 115 covered entities' HIPAA compliance controls and processes
- Phase 2 announced March 21, 2016
  - Includes *both* covered entities and business associates

Phase 2 Audit Structure

- Purpose to assess HIPAA compliance over wide range of entities
  - Examine compliance mechanisms
  - Identify best practices
  - Discover risks and vulnerabilities
- Provide guidance based on findings
- Enhanced audit protocols

Scope of Phase 2 OCR Audits

2016 Desk Audits of Covered Entities

- Security - Risk Analysis and risk management
- Breach - Content and timeliness of breach notifications
- Privacy - Notice of Privacy Practices and Access

2016 Desk Audits of Business Associates

- Security - Risk Analysis and risk management
- Breach - Breach reporting to covered entities

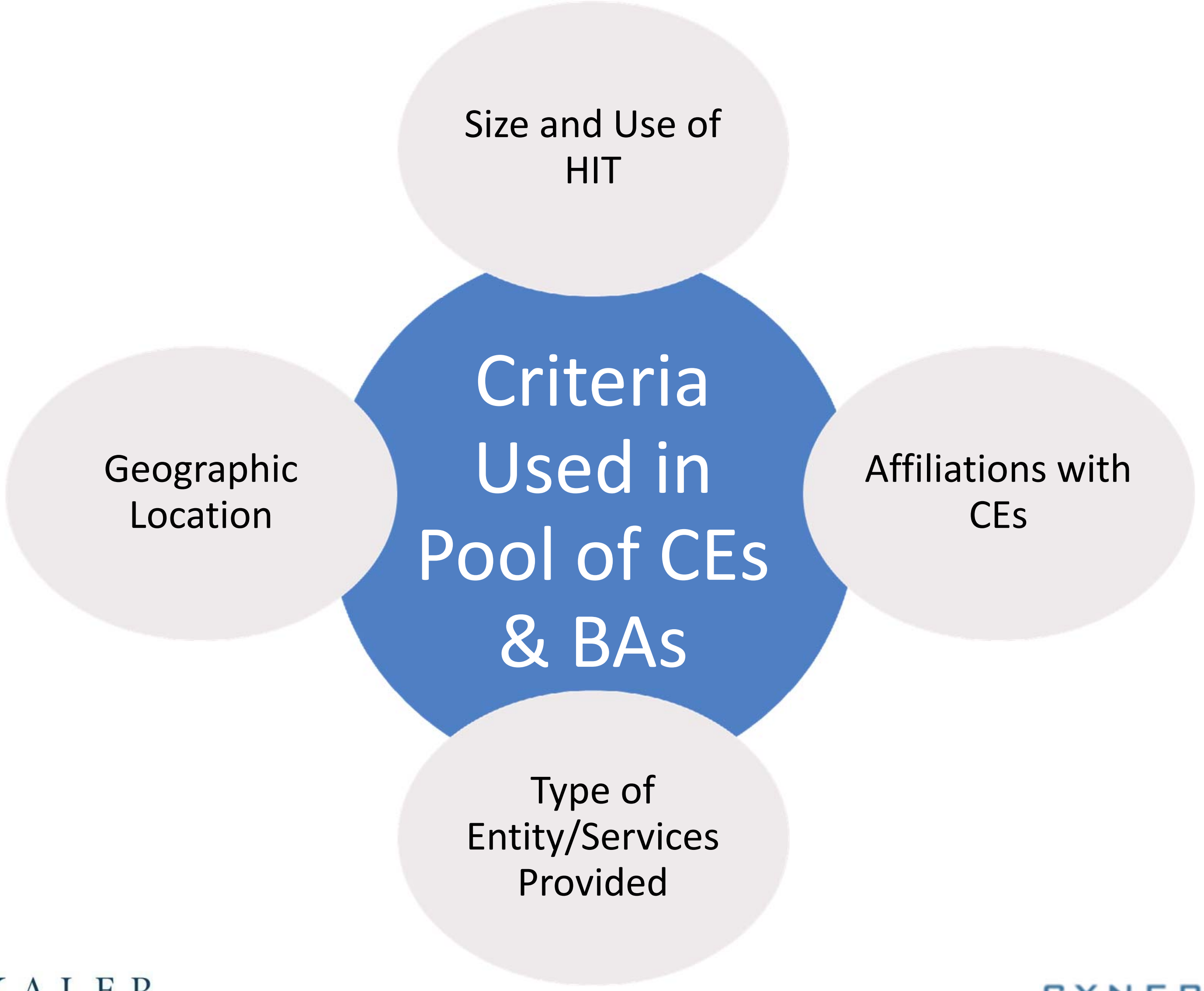
2016-17 On-site Comprehensive Audits

- Covered entities
- Business associates

Phase 2 Audits - Who?

- Every covered entity and business associate is subject to audit, so remember -
  - Covered entities are not just providers = health plans, clearinghouses, too
  - Business associates include subcontractor business associates
- Diverse group to be selected
- Low risk / high impact
- Entities under current OCR review will not be selected for audit

Phase 2 Audit Selection Criteria



Criteria Used in Pool of CEs & BAs

Size and Use of HIT

Geographic Location

Affiliations with CEs

Type of Entity/Services Provided

Phase 2 Audits – Preparation

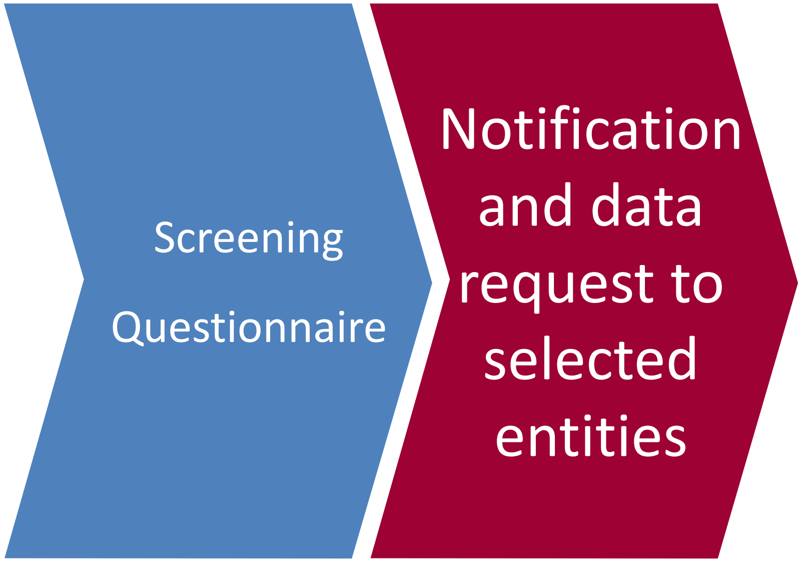
- Identify core "audit response team"
  - Ensure privacy officer has heightened awareness regarding OCR email notice
  - May be overlooked or filtered as Spam (OSOCRAudit@hhs.gov)
  - *See sample letter at end*
  - Identify those responsible within the process
  - If they are out of the office, have a back up plan
- Provide training on audit response
- Prepare for audit using OCR's sample audit protocol

Phase 2 Audits – The Desk Audit Steps

Screening Questionnaire

- Contact information requested
- Collected information helps create pool of potential auditees
  - See *sample questionnaire at end*
- Not responding ≠ Getting off the Hook
  - OCR will use public information to create the pool from which selected auditees are randomly chosen
  - Ensure such information is updated (Medicare enrollment, state licensure, websites)
  - May result in OCR compliance review

Phase 2 Audits – The Desk Audit Steps

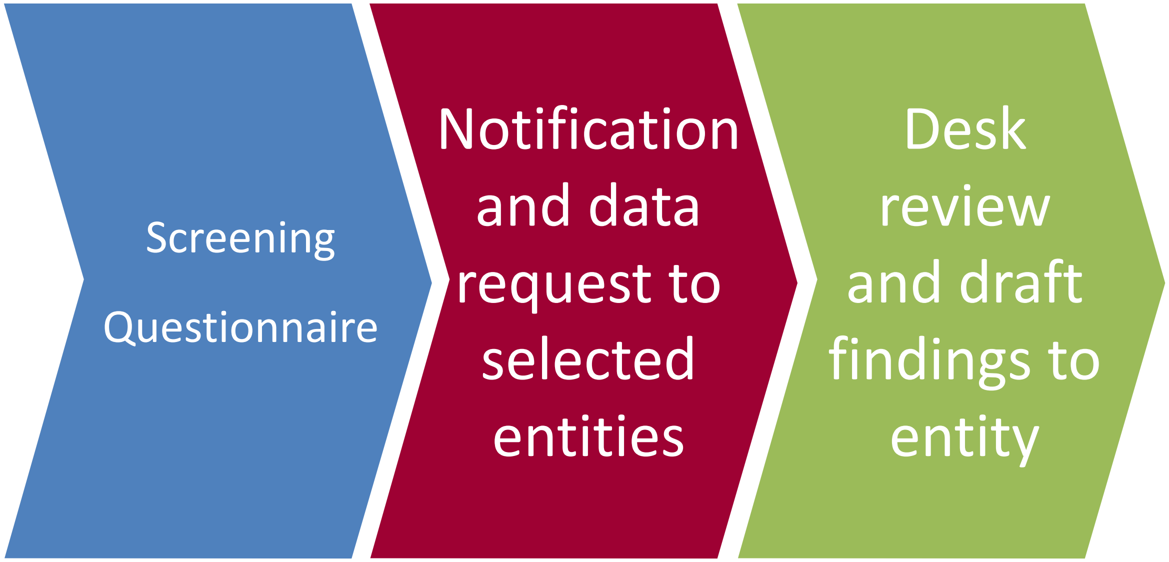


- Auditee notified of selection
- Data requests
- Ensure relevant information is current and available
- Data may be required within 10 days of request

Phase 2 Audits – How to Prepare

- Covered Entities will be asked to identify their business associates
  - Ensure Business Associate Agreements are current
  - OCR’s sample template business associate list is not required, but same data must be provided (24 data points)
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
- Review policies to ensure they are implemented
- Review prior breach notices to ensure compliance with requirements
- Have all documentation in centralized and easy to find location

Phase 2 Audits - The Desk Audit Steps



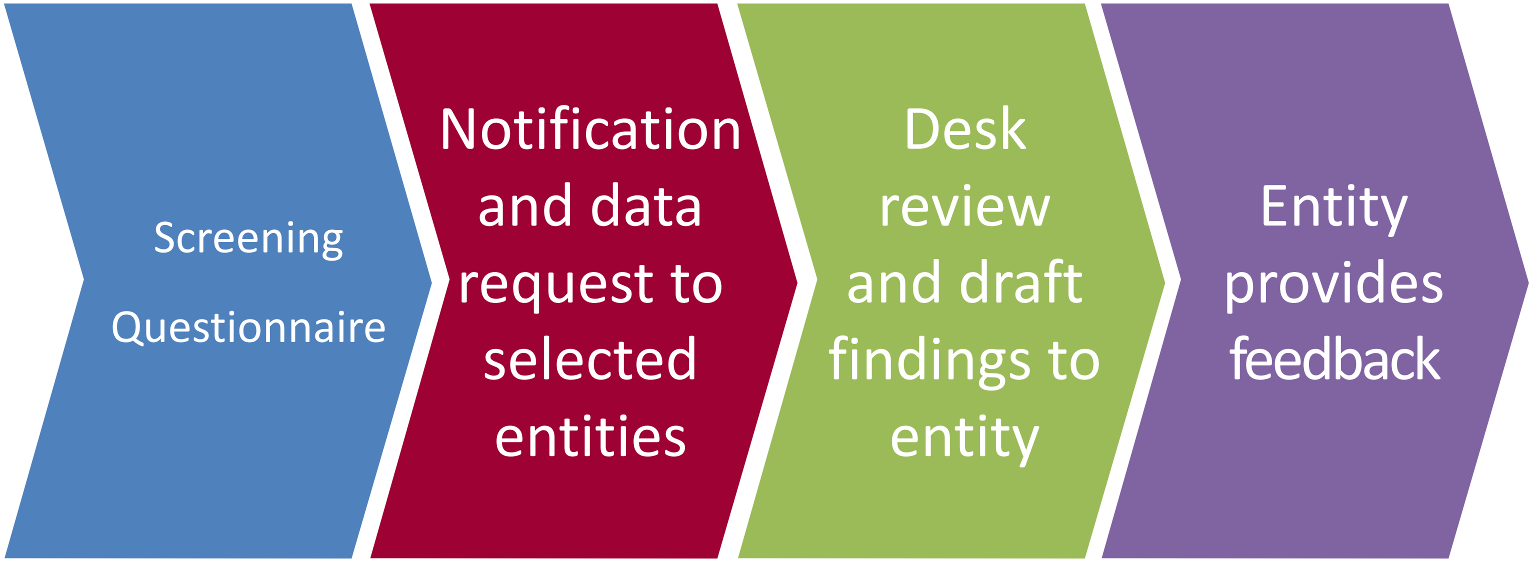
Screening Questionnaire

Notification and data request to selected entities

Desk review and draft findings to entity

- Desk audits to be completed by December 2016
- Draft findings submitted to CE or BA
- Time frame in which CMS must prepare draft findings is not known

Phase 2 Audits – The Desk Audit Steps



Screening Questionnaire

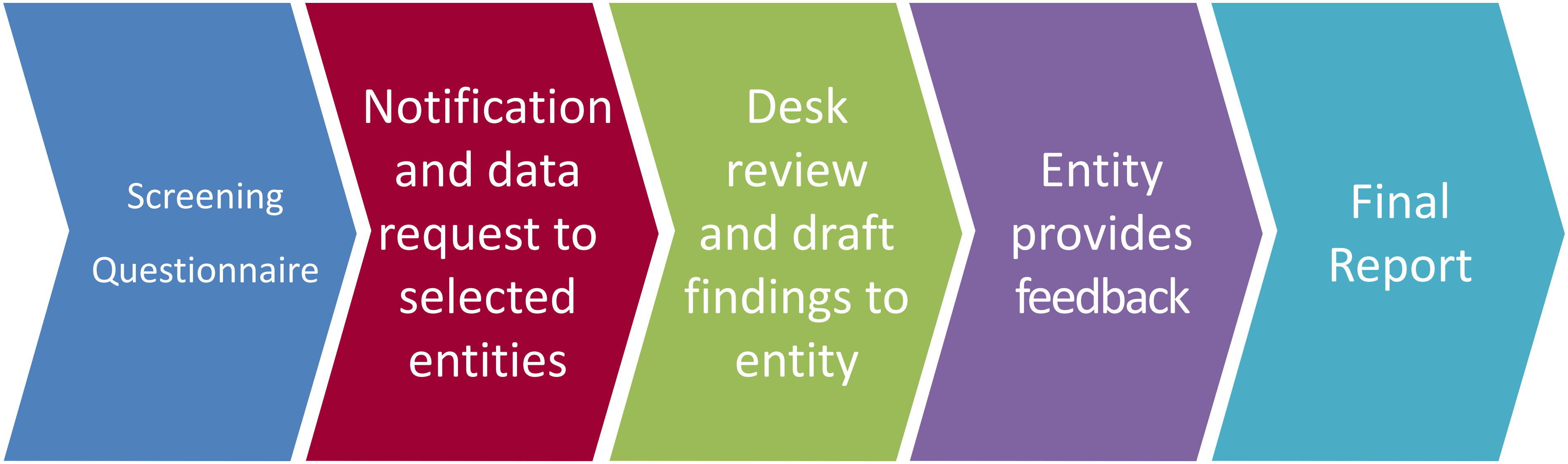
Notification and data request to selected entities

Desk review and draft findings to entity

Entity provides feedback

- CE or BA may respond to draft findings
- Must do so in 10 days
- Responses will be incorporated into final report

Phase 2 Audits – The Desk Audit Steps


Screening Questionnaire
Notification and data request to selected entities
Desk review and draft findings to entity
Entity provides feedback
Final Report

- OCR has 30 days from receiving responses to prepare report
- Final report will be shared with CE or BA

Phase 2 – Audits

Onsite Audits

Phase 2 Audits – Onsite Audits

- 2016-2017 audits
- Process and time lines for desk audits will be followed for onsite audits
- Entrance conference
- Three to five days in length
- More comprehensive than the desk audits
- No end date identified

Phase 2 Audits – Onsite Audits

- Conducted in accordance with Generally Accepted Government Audit Standards (GAGAS)
- Provides findings, observations, or conclusions from evaluation of evidence against established criteria
- Objective assessment of variety of attributes
  - Program effectiveness, economy, and efficiency
  - Internal controls
  - Compliance

Scope of OCR Onsite Audits

Security

- Device and media controls
- Transmission security
- Encryption of data at rest
- Facility access controls

Privacy

- Administrative and physical safeguards
- Workforce training to HIPAA policies & procedures
- Individual access to PHI in electronic format

Other Areas

- High risk areas identified through:
  - 2016 desk audits
  - Breach reports submitted to OCR
  - Consumer complaints

Scope of Future OCR Onsite Audits

Security

- Device and media controls
- Transmission security
- Encryption of data at rest
- Facility access controls

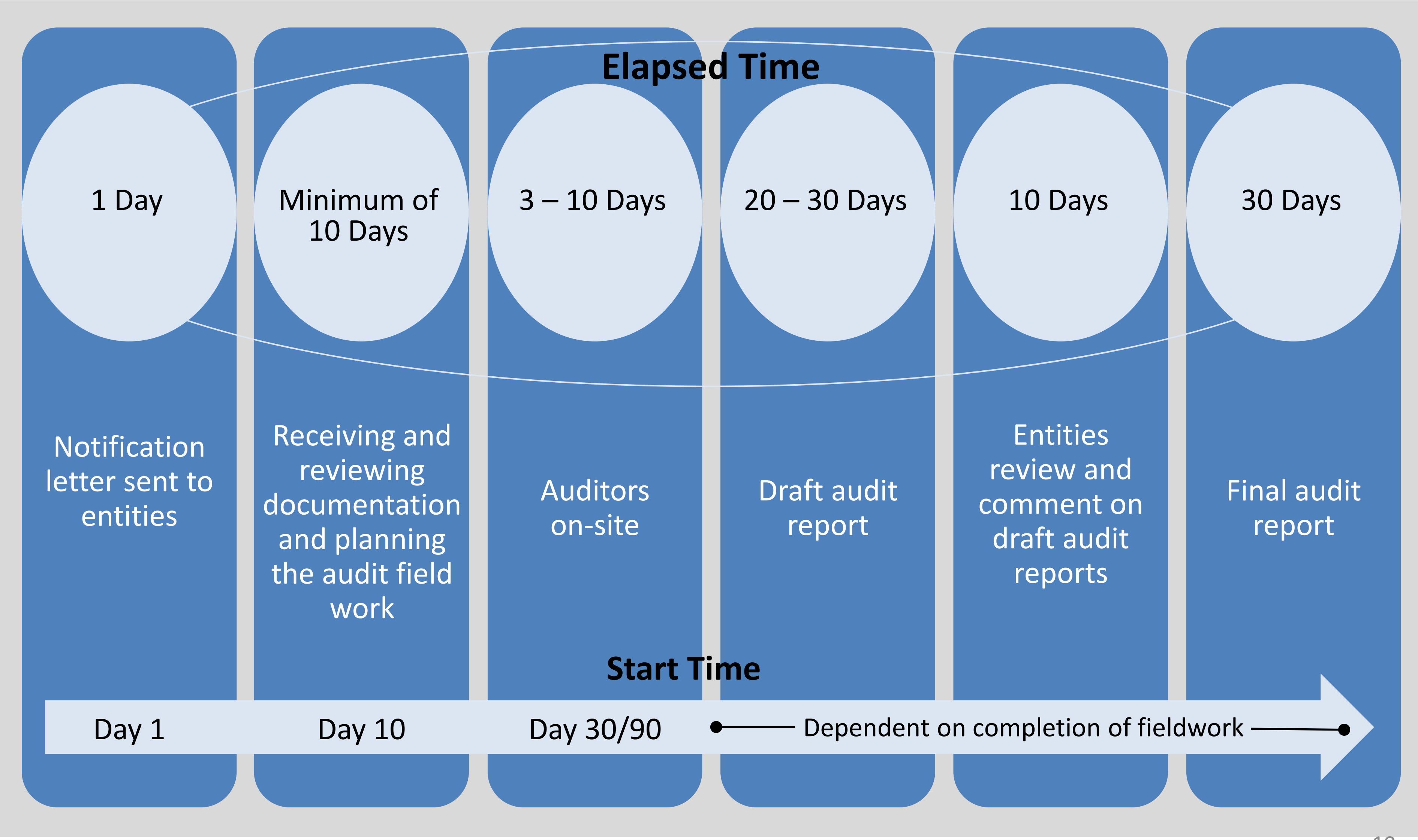
Privacy

- Administrative and physical safeguards
- Workforce training to HIPAA policies & procedures
- Individual access to PHI in electronic format

Other Areas

- High risk areas identified through:
  - 2016 desk audits
  - Breach reports submitted to OCR
  - Consumer complaints

Phase 2 - Comprehensive On-Site Audit Process



Elapsed Time
1 Day
Minimum of 10 Days
3 – 10 Days
20 – 30 Days
10 Days
30 Days
Notification letter sent to entities
Receiving and reviewing documentation and planning the audit field work
Auditors on-site
Draft audit report
Entities review and comment on draft audit reports
Final audit report
Start Time
Day 1
Day 10
Day 30/90
Dependent on completion of fieldwork

Phase 2 Audits - Sample Comprehensive On-Site Audit Protocol - Provider

Breach Notification

- Assessment for breach
- Notification to individuals
- Notification to Secretary
- Notification to media

Privacy

- Notice of Privacy Practices
- Request Restrictions
- Right to Access
- Administrative Requirements
- Amendment
- Uses & Disclosures
- Accounting of Disclosures

Security

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Phase 2 – Post-Audit

Phase 2 Audits – Post-Audit

- OCR will use findings to develop more assistance for covered entities and business associates for use in their HIPAA compliance activities

- If serious issues identified, OCR may initiate a compliance review

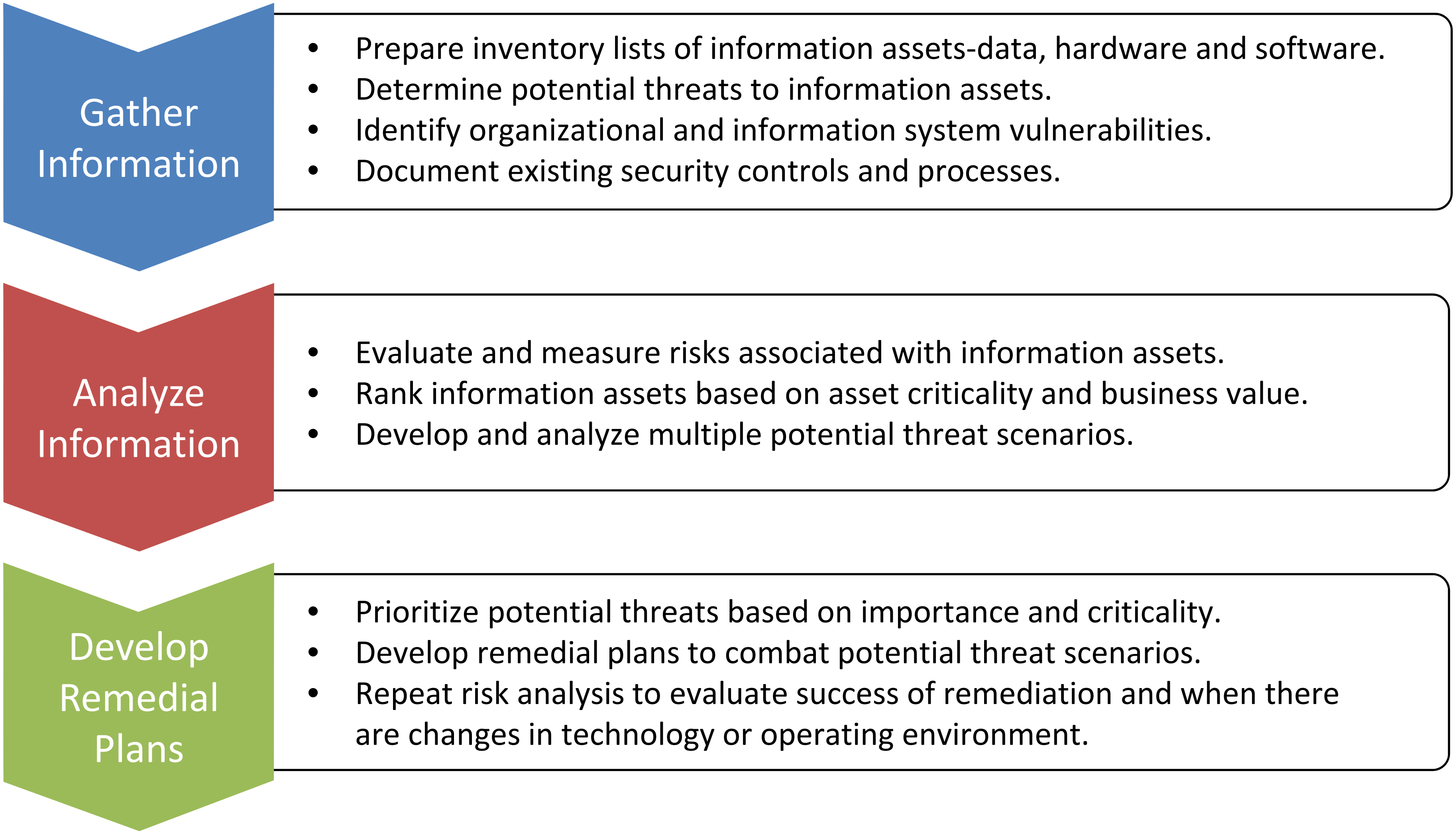
- OCR will not post list of auditees or audit findings but may be required to disclose via a FOIA request
  - Important for covered entities to thoughtfully respond to audit findings

CREATING AN OCR AUDIT TOOLKIT

Phase 2 Audits – HIPAA Security Risk Assessment

- Required element for Security Rule and Meaningful Use
- An assessment of threats and vulnerabilities to information systems that handle e-PHI
- This provides the starting point for determining what is ‘**appropriate**’ and ‘**reasonable**’
- Organizations determine their own technology and administrative choices to mitigate their risks
- The risk analysis process should be ongoing and repeated as needed when the organization experiences changes in technology or operating environment

Phase 2 Audits – Performing a Risk Analysis



Gather Information

- Prepare inventory lists of information assets-data, hardware and software.
- Determine potential threats to information assets.
- Identify organizational and information system vulnerabilities.
- Document existing security controls and processes.

Analyze Information

- Evaluate and measure risks associated with information assets.
- Rank information assets based on asset criticality and business value.
- Develop and analyze multiple potential threat scenarios.

Develop Remedial Plans

- Prioritize potential threats based on importance and criticality.
- Develop remedial plans to combat potential threat scenarios.
- Repeat risk analysis to evaluate success of remediation and when there are changes in technology or operating environment.

Phase 2 Audits – Building an Audit Tool Kit

- Prepare a plan to perform mock audits
- Replicate what documentation would be required under audit conditions and the timelines for production
- Use OCR’s 2016 Phase 2 HIPAA Audit Protocol
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
- Use the results from your audit to develop a work plan for policies and processes that should be reviewed or updated

Example: Security Management Process

Key Activity	Established Performance Criteria	Audit Inquiry
Security Management Process	§164.308(a): A covered entity or business associate must in accordance with 164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.	Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations? Does the entity prevent, detect, contain and correction security violations? Obtain and review policies and procedures related to security violations. Evaluate the content relative to the specified performance criteria for countermeasures or safeguards implemented to prevent, detect, contain and correct security violations. Obtain and review documentation demonstrating that policies and procedures have been implemented to prevent, detect, contain, correct security violations. Evaluate and determine if the process used is in accordance with related policies and procedures. Obtain and review documentation of security violations and remediation actions. Evaluate and determine if security violations where handled in accordance with the related policies and procedures; safeguards or countermeasures to prevent violations from occurring; identify and characterize violations as they happen; limit the extent of any damages caused by violations; have corrective action plan in place to manage risk.

Example: Encryption and Decryption

Key Activity	Established Performance Criteria	Audit Inquiry
Access Control -- Encryption and Decryption	§164.312(a)(2)(iv): Implement a mechanism to encrypt and decrypt electronic protected health information.	Does the entity have policies and procedures in place to encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI? Does the entity encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI? Obtain and review the policies and procedures regarding the encryption and decryption of ePHI. Evaluate the content relative to the specified criteria to determine that the implementation and use of encryption appropriately protects ePHI. Obtain and review documentation demonstrating ePHI being encrypted and decrypted. Evaluate and determine if ePHI is encrypted and decrypted in accordance with related policies and procedures. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Example: Required by Law Disclosures

Key Activity	Established Performance Criteria	Audit Inquiry
Uses and disclosures required by law	§164.512(a)(1) - A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies and is limited to the relevant requirements of such law. §164.512(a)(2) - A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.	Does the entity have policies and procedures in place to encrypt Does the covered entity use and disclose PHI pursuant to requirements of other law? If so, are such uses and disclosures made consistent with the requirements of this performance criterion as well as the applicable requirements related to victims of abuse, neglect or domestic violence, pursuant to judicial and administrative proceedings and law enforcement purposes of this section? Obtain and review policies and procedures for uses and disclosures required by law.

Example: Privacy Breach Rule Training

Key Activity	Established Performance Criteria	Audit Inquiry
Training	§164.530(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 and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. (2) Implementation specifications: Training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows: (A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity; (B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and (C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section. (ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.	Does the covered entity train its work force and have a policies and procedures to ensure all members of the workforce receive necessary and appropriate training in a timely manner as provided for by the established performance criterion? Obtain and review such policies and procedures. Areas to review include training each new member of the workforce within a reasonable period of time and each member whose functions are affected by a material change in policies or procedures. From the population of new hires within the audit period, obtain and review a sample of documentation of necessary and appropriate training on the HIPAA Privacy Rule that has been provided and completed. Obtain and review documentation that workforce members have been trained on material changes to policies and procedures required by the HITECH Act.

Example: Notice to Individuals

Key Activity	Established Performance Criteria	Audit Inquiry
Notice to Individuals of Breach	§164.404(a)(1) Notice to Individuals. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Does the covered entity have policies and procedures for notifying individuals of a breach of their protected health information. Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the affected individuals. Determine whether notifications were provided to individuals consistent with the requirements in §164.404(a)(1).

Questions?

Type your questions into
the Questions pane.

We’ll answer as many as we can.

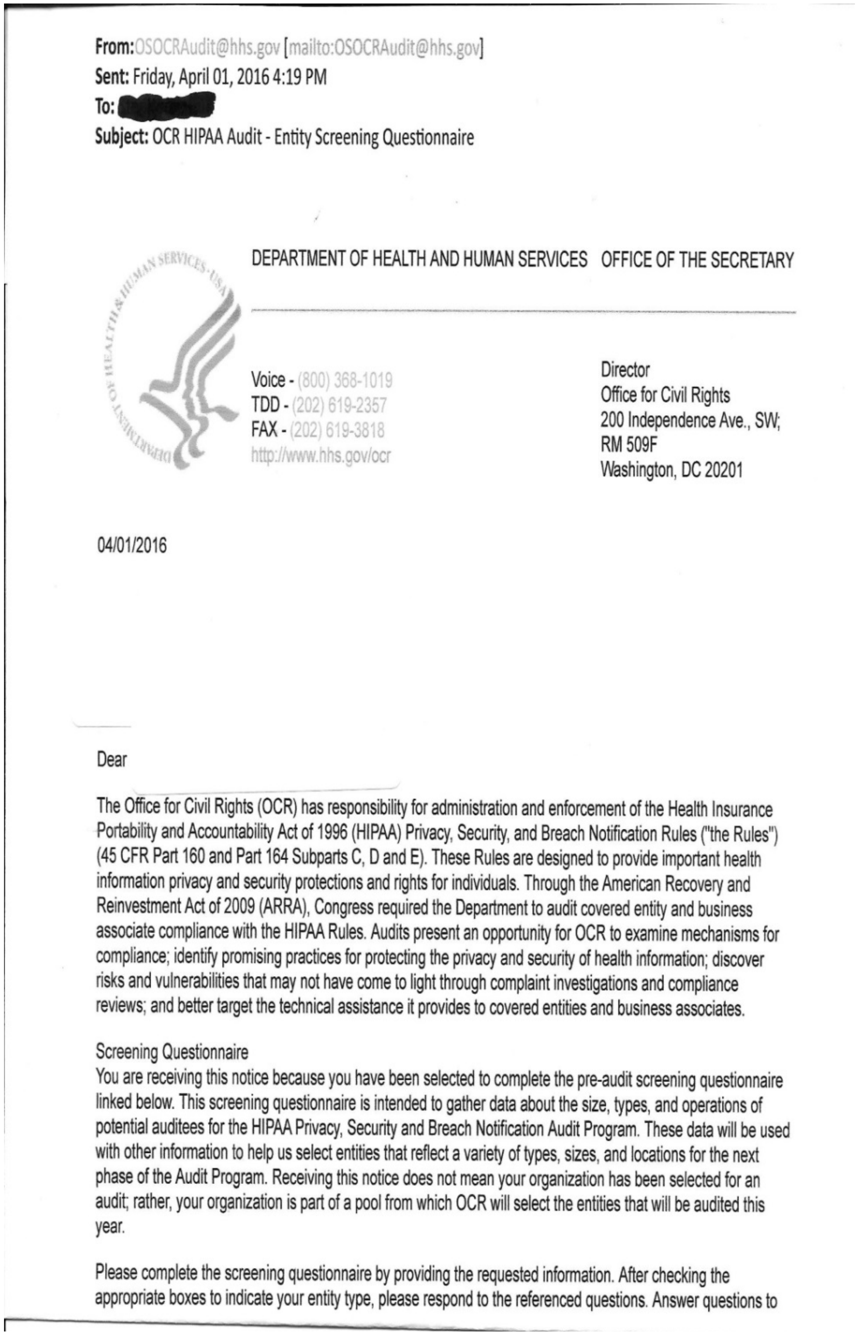
More Questions? Contact Us.

James B. Wieland
Principal
Ober|Kaler
jbwieland@ober.com

Emily H. Wein
Principal
Ober|Kaler
ehwein@ober.com

David Holtzman
Vice President of Compliance Services,
CynergisTek, Inc.
david.holtzman@cynergistek.com
@HITprivacy

Sample Audit Letter and Attached questionnaire



From: OSOCRAudit@hhs.gov [mailto:OSOCRAudit@hhs.gov]
Sent: Friday, April 01, 2016 4:19 PM
To: [redacted]
Subject: OCR HIPAA Audit - Entity Screening Questionnaire

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice - (800) 368-1019
TDD - (202) 619-2357
FAX - (202) 619-3818
http://www.hhs.gov/ocr

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

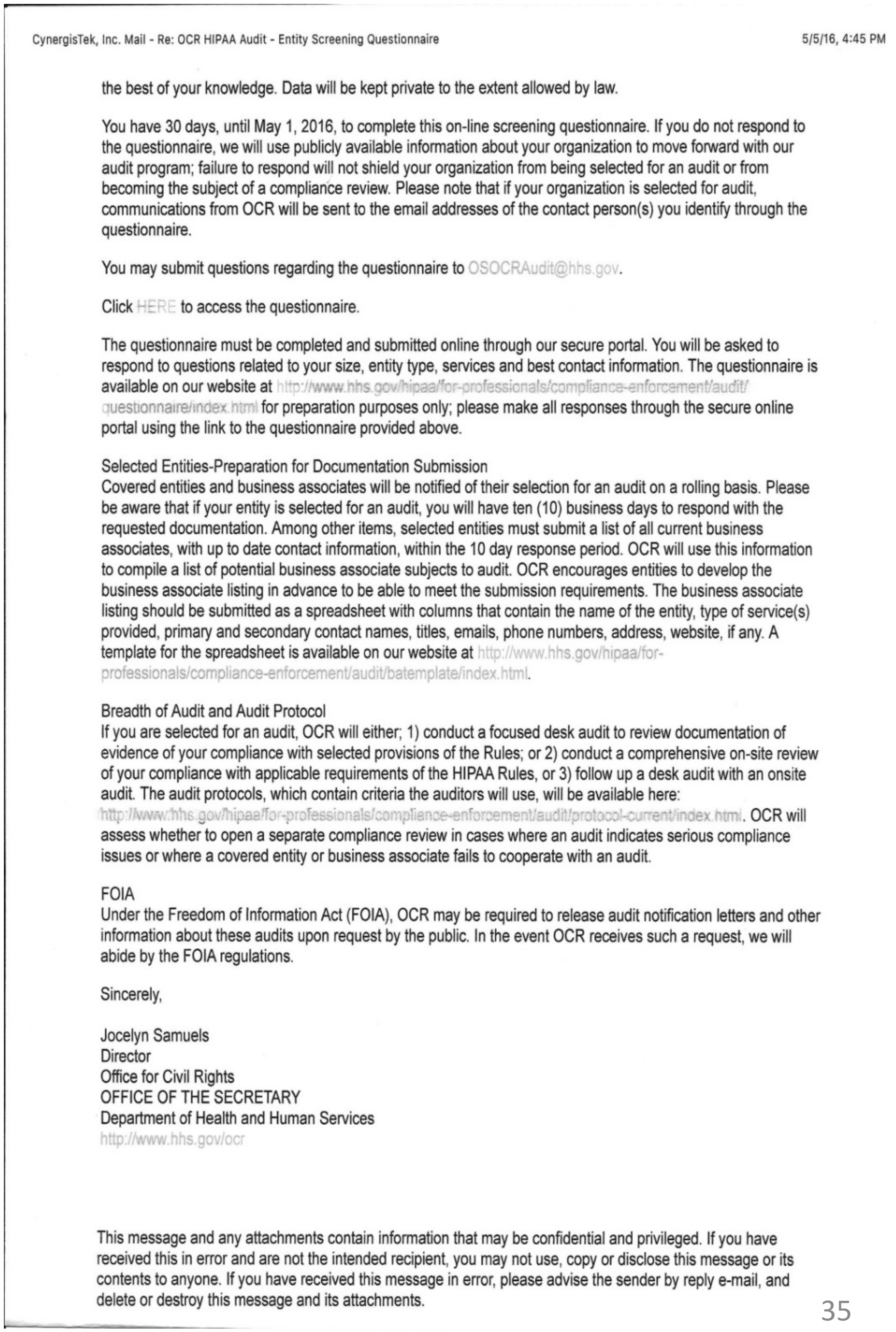
04/01/2016

Dear

The Office for Civil Rights (OCR) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules ("the Rules") (45 CFR Part 160 and Part 164 Subparts C, D and E). These Rules are designed to provide important health information privacy and security protections and rights for individuals. Through the American Recovery and Reinvestment Act of 2009 (ARRA), Congress required the Department to audit covered entity and business associate compliance with the HIPAA Rules. Audits present an opportunity for OCR to examine mechanisms for compliance; identify promising practices for protecting the privacy and security of health information; discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews; and better target the technical assistance it provides to covered entities and business associates.

Screening Questionnaire
You are receiving this notice because you have been selected to complete the pre-audit screening questionnaire linked below. This screening questionnaire is intended to gather data about the size, types, and operations of potential auditees for the HIPAA Privacy, Security and Breach Notification Audit Program. These data will be used with other information to help us select entities that reflect a variety of types, sizes, and locations for the next phase of the Audit Program. Receiving this notice does not mean your organization has been selected for an audit; rather, your organization is part of a pool from which OCR will select the entities that will be audited this year.

Please complete the screening questionnaire by providing the requested information. After checking the appropriate boxes to indicate your entity type, please respond to the referenced questions. Answer questions to



the best of your knowledge. Data will be kept private to the extent allowed by law.

You have 30 days, until May 1, 2016, to complete this on-line screening questionnaire. If you do not respond to the questionnaire, we will use publicly available information about your organization to move forward with our audit program; failure to respond will not shield your organization from being selected for an audit or from becoming the subject of a compliance review. Please note that if your organization is selected for audit, communications from OCR will be sent to the email addresses of the contact person(s) you identify through the questionnaire.

You may submit questions regarding the questionnaire to OSOCRAudit@hhs.gov.

Click HERE to access the questionnaire.

The questionnaire must be completed and submitted online through our secure portal. You will be asked to respond to questions related to your size, entity type, services and best contact information. The questionnaire is available on our website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html for preparation purposes only; please make all responses through the secure online portal using the link to the questionnaire provided above.

Selected Entities-Preparation for Documentation Submission
Covered entities and business associates will be notified of their selection for an audit on a rolling basis. Please be aware that if your entity is selected for an audit, you will have ten (10) business days to respond with the requested documentation. Among other items, selected entities must submit a list of all current business associates, with up to date contact information, within the 10 day response period. OCR will use this information to compile a list of potential business associate subjects to audit. OCR encourages entities to develop the business associate listing in advance to be able to meet the submission requirements. The business associate listing should be submitted as a spreadsheet with columns that contain the name of the entity, type of service(s) provided, primary and secondary contact names, titles, emails, phone numbers, address, website, if any. A template for the spreadsheet is available on our website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html.

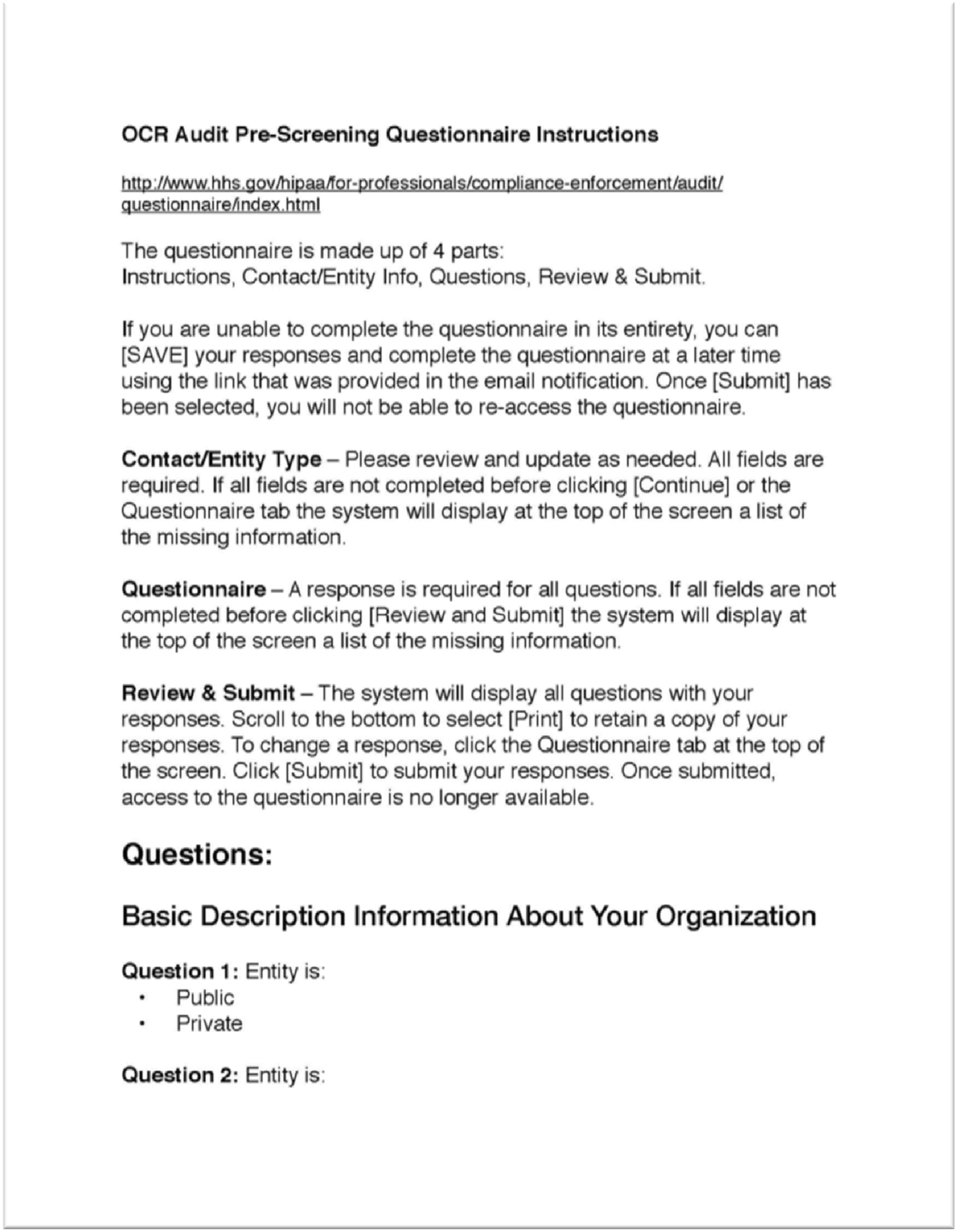
Breadth of Audit and Audit Protocol
If you are selected for an audit, OCR will either; 1) conduct a focused desk audit to review documentation of evidence of your compliance with selected provisions of the Rules; or 2) conduct a comprehensive on-site review of your compliance with applicable requirements of the HIPAA Rules, or 3) follow up a desk audit with an onsite audit. The audit protocols, which contain criteria the auditors will use, will be available here: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html. OCR will assess whether to open a separate compliance review in cases where an audit indicates serious compliance issues or where a covered entity or business associate fails to cooperate with an audit.

FOIA
Under the Freedom of Information Act (FOIA), OCR may be required to release audit notification letters and other information about these audits upon request by the public. In the event OCR receives such a request, we will abide by the FOIA regulations.

Sincerely,

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

This message and any attachments contain information that may be confidential and privileged. If you have received this in error and are not the intended recipient, you may not use, copy or disclose this message or its contents to anyone. If you have received this message in error, please advise the sender by reply e-mail, and delete or destroy this message and its attachments.



OCR Audit Pre-Screening Questionnaire Instructions

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

The questionnaire is made up of 4 parts:
Instructions, Contact/Entity Info, Questions, Review & Submit.

If you are unable to complete the questionnaire in its entirety, you can [SAVE] your responses and complete the questionnaire at a later time using the link that was provided in the email notification. Once [Submit] has been selected, you will not be able to re-access the questionnaire.

Contact/Entity Type – Please review and update as needed. All fields are required. If all fields are not completed before clicking [Continue] or the Questionnaire tab the system will display at the top of the screen a list of the missing information.

Questionnaire – A response is required for all questions. If all fields are not completed before clicking [Review and Submit] the system will display at the top of the screen a list of the missing information.

Review & Submit – The system will display all questions with your responses. Scroll to the bottom to select [Print] to retain a copy of your responses. To change a response, click the Questionnaire tab at the top of the screen. Click [Submit] to submit your responses. Once submitted, access to the questionnaire is no longer available.

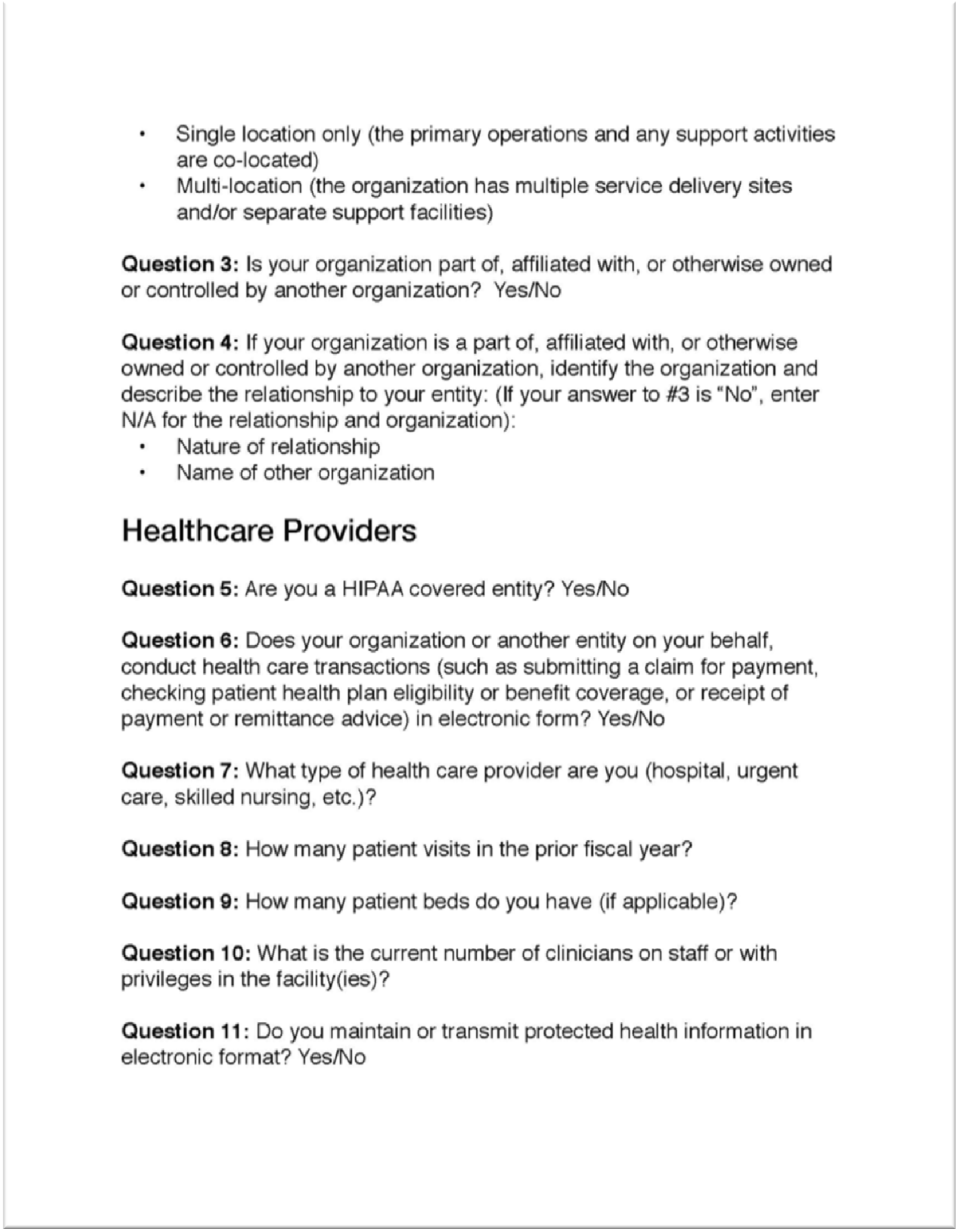
Questions:

Basic Description Information About Your Organization

Question 1: Entity is:

- Public
- Private

Question 2: Entity is:



- Single location only (the primary operations and any support activities are co-located)
- Multi-location (the organization has multiple service delivery sites and/or separate support facilities)

Question 3: Is your organization part of, affiliated with, or otherwise owned or controlled by another organization? Yes/No

Question 4: If your organization is a part of, affiliated with, or otherwise owned or controlled by another organization, identify the organization and describe the relationship to your entity: (If your answer to #3 is "No", enter N/A for the relationship and organization):

- Nature of relationship
- Name of other organization

Healthcare Providers

Question 5: Are you a HIPAA covered entity? Yes/No

Question 6: Does your organization or another entity on your behalf, conduct health care transactions (such as submitting a claim for payment, checking patient health plan eligibility or benefit coverage, or receipt of payment or remittance advice) in electronic form? Yes/No

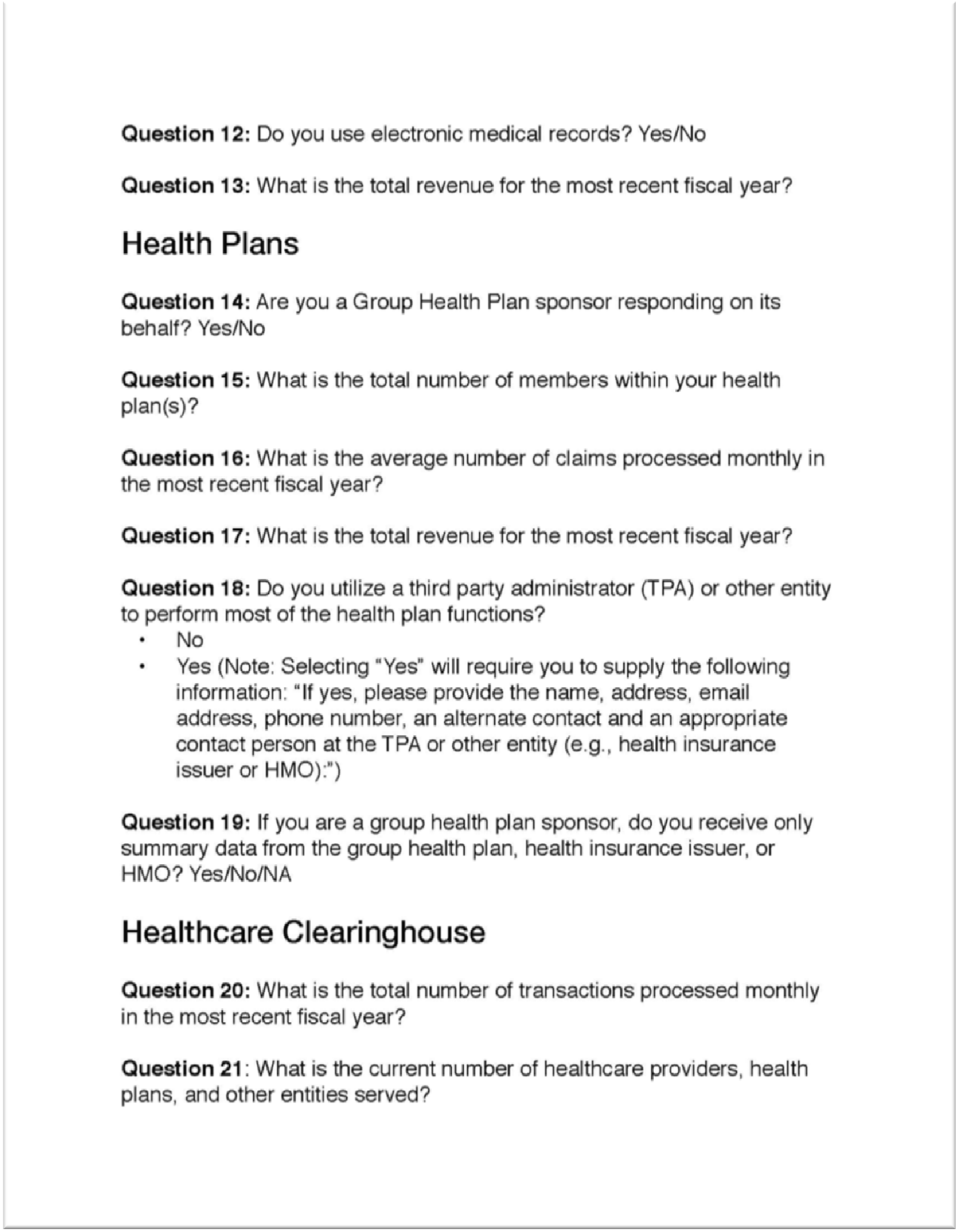
Question 7: What type of health care provider are you (hospital, urgent care, skilled nursing, etc.)?

Question 8: How many patient visits in the prior fiscal year?

Question 9: How many patient beds do you have (if applicable)?

Question 10: What is the current number of clinicians on staff or with privileges in the facility(ies)?

Question 11: Do you maintain or transmit protected health information in electronic format? Yes/No



Question 12: Do you use electronic medical records? Yes/No

Question 13: What is the total revenue for the most recent fiscal year?

Health Plans

Question 14: Are you a Group Health Plan sponsor responding on its behalf? Yes/No

Question 15: What is the total number of members within your health plan(s)?

Question 16: What is the average number of claims processed monthly in the most recent fiscal year?

Question 17: What is the total revenue for the most recent fiscal year?

Question 18: Do you utilize a third party administrator (TPA) or other entity to perform most of the health plan functions?

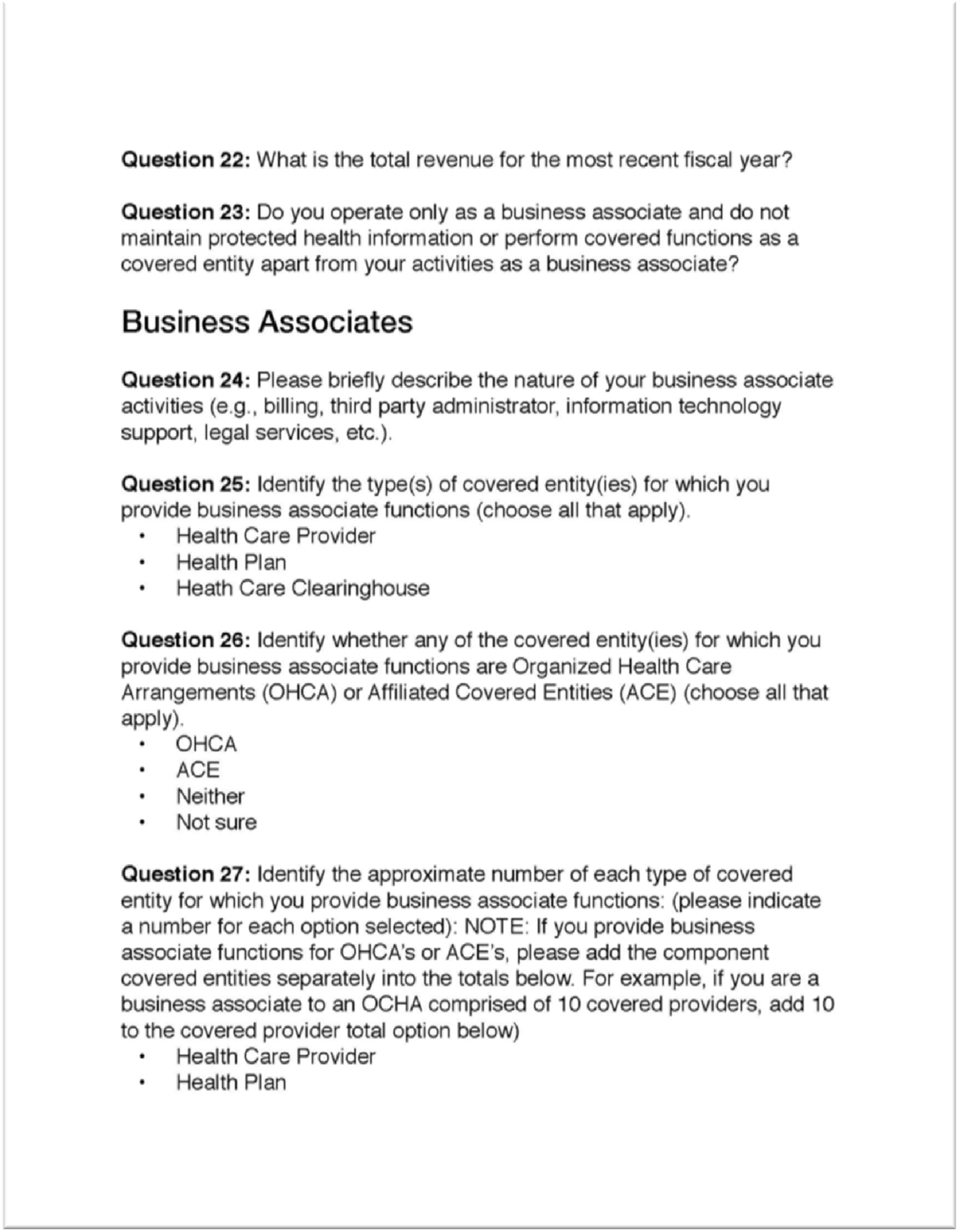
- No
- Yes (Note: Selecting "Yes" will require you to supply the following information: "If yes, please provide the name, address, email address, phone number, an alternate contact and an appropriate contact person at the TPA or other entity (e.g., health insurance issuer or HMO):")

Question 19: If you are a group health plan sponsor, do you receive only summary data from the group health plan, health insurance issuer, or HMO? Yes/No/NA

Healthcare Clearinghouse

Question 20: What is the total number of transactions processed monthly in the most recent fiscal year?

Question 21: What is the current number of healthcare providers, health plans, and other entities served?



Question 22: What is the total revenue for the most recent fiscal year?

Question 23: Do you operate only as a business associate and do not maintain protected health information or perform covered functions as a covered entity apart from your activities as a business associate?

Business Associates

Question 24: Please briefly describe the nature of your business associate activities (e.g., billing, third party administrator, information technology support, legal services, etc.).

Question 25: Identify the type(s) of covered entity(ies) for which you provide business associate functions (choose all that apply).

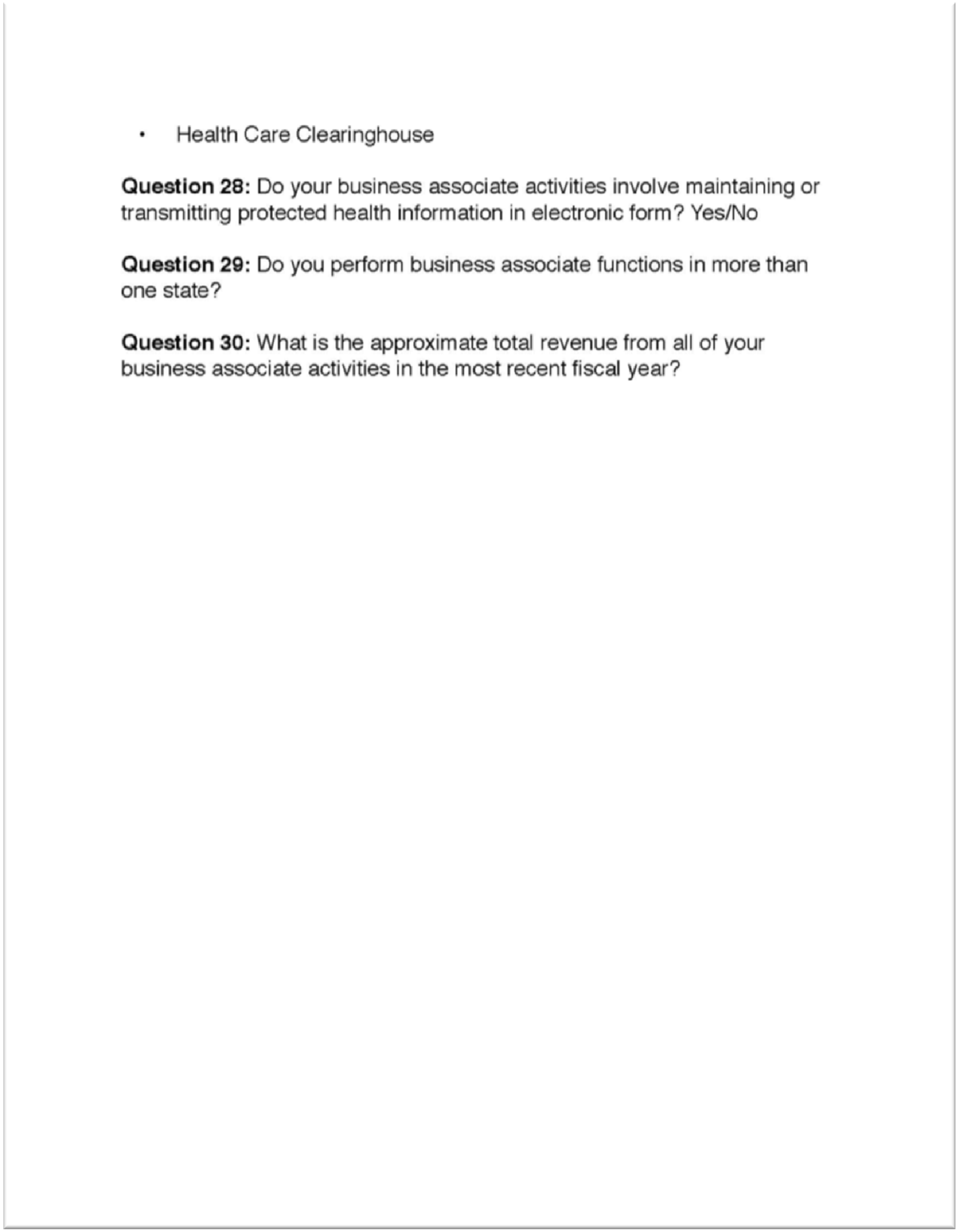
- Health Care Provider
- Health Plan
- Heath Care Clearinghouse

Question 26: Identify whether any of the covered entity(ies) for which you provide business associate functions are Organized Health Care Arrangements (OHCA) or Affiliated Covered Entities (ACE) (choose all that apply).

- OHCA
- ACE
- Neither
- Not sure

Question 27: Identify the approximate number of each type of covered entity for which you provide business associate functions: (please indicate a number for each option selected): NOTE: If you provide business associate functions for OHCA's or ACE's, please add the component covered entities separately into the totals below. For example, if you are a business associate to an OCHA comprised of 10 covered providers, add 10 to the covered provider total option below)

- Health Care Provider
- Health Plan



- Health Care Clearinghouse

Question 28: Do your business associate activities involve maintaining or transmitting protected health information in electronic form? Yes/No

Question 29: Do you perform business associate functions in more than one state?

Question 30: What is the approximate total revenue from all of your business associate activities in the most recent fiscal year?