HIPAA PRIVACY, SECURITY & BREACH NOTIFICATION COMPLIANCE AUDITS PHASE 2

INFORMATIONAL WEBINAR

Wednesday, July 13, 2016

Jocelyn Samuels, JD, Director

Deven McGraw, JD, HIP Division Deputy Director

Linda Sanches, MPH

Zinethia L. Clemmons, MBA, MHA, RHIA, PMP

Department of Health and Human Services

Office for Civil Rights

PART I: PURPOSE OF WEBINAR

On July 11, 2016 OCR notified 167 Covered Entities of selection to participate in the HIPAA desk audits

This webinar will:

- Discuss the desk audit process
- Identify expectations
- Give the auditees an opportunity to ask questions and raise concerns

WEBINAR AGENDA

- Opening remarks—Jocelyn Samuels
- Introduction
  - Phase II HIPAA Audit Program
  - Random Selection Process
  - Desk Audits vs. Onsite Audits
- Desk Audit Mechanics
  - What to Expect
  - Subject HIPAA Controls
  - Document Request – Receipt and Response
  - Final Reports
- Walk through document submission requirements
- Q&A's

WELCOMING REMARKS

Jocelyn Samuels

PHASE II HIPAA AUDIT OVERVIEW

OCR conducted its first audits in 2012. They were comprehensive, on-site audits of the compliance activities of 115 covered entities. The program has been redesigned to reflect an evaluation and new law

Phase II will:

- Include both covered entities and business associates
- Be comprised of 200-250 audits in total
  - Over 200 desk audits
  - Smaller number of comprehensive on-site audits

Phase II designed to enable OCR to examine mechanisms for compliance

- Identify industry best practices
- Discover risks and vulnerabilities not surfaced through enforcement activities
- Enable us to get out in front of problems before they result in breaches

AUDIT REPORTING OCR GOALS

Audits primarily a compliance improvement activity to help OCR to

- better understand compliance efforts with particular aspects of the HIPAA Rules.
- determine what types of technical assistance OCR should develop
- develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches.

OCR will not post a listing of audited entities or entity-identified findings. However, 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

SELECTION PROCESS

- OCR identified pools of CEs that represent a wide range of health care providers, health plans, health care clearinghouses, to better assess HIPAA compliance across the industry.
- Sampling criteria included size, affiliations, location, public or private,…
- Health plans were divided into **group plans** and **issuers** and providers were further categorized by type
  - hospital, practitioner, elder care/SNF, health system, pharmacy
- OCR then ran a randomized selection algorithm that drew from each of the categories, resulting in 167 CEs.
- Finally, the auditees were checked for conflict of interests with the contractor supporting OCR in the audit process, as well as subjects of ongoing investigations. Conflicting auditees were replaced in kind

DESK AUDITS NOW, ONSITE AUDITS LATER

- The covered entity desk audits are now underway, and will continue through the end of the year
- Desk audit scope is limited to a total of 7 controls drawn from the Security Rule, the Privacy Rule, and the Breach Notification Rule. **Entities will either be audited on SR controls or PR & BNR compliance**
- Onsite audits will begin in early 2017
- Onsite audits will evaluate auditees against comprehensive set of HIPAA compliance controls.
- A desk auditee subject may be subject to an onsite audit

PART II: DESK AUDIT MECHANICS

- What to expect
- Timeline for responding to document requests
- OCR's expectations regarding document response submissions
- The specific HIPAA controls subject to the desk audits
- The Final Report procedures

WHAT TO EXPECT

Covered entities have 10 business days (until July 22, 2016) to provide their responses

- Responses should contain the specified documentation-- applicable policies, procedures, evidence of implementation
- Provide complete and relevant materials
- Refrain from submitting superfluous documentation! 10MB file size limitation--

The desk audits of BAs will commence in late September.

- The same rules and expectations apply to the BA auditees The selection pool of the BAs largely drawn from the BAs identified by CEs

DOCUMENT REQUESTS & RESPONSES TIMELINE

The document request

- Sent to selected auditees via email
- Comprised of **two** separate requests
  - one listing policies, procedures, and/or other related documentation
  - one requesting a list of all the CE's BAs
- Specify the documentation elements to be provided
- Note that BA listings must be returned **electronically, via email**, to OCR within 10 business days
- All other items must be submitted using the secure online portal link provided in the notification email

DOCUMENT REQUESTS & RESPONSES EXPECTATIONS

Depending on the type of entity, each auditee is expected to:

- Provide **only** the policies and procedures that are relevant to the controls requested
  - E.g., CEs must extract the relevant language from larger compendiums of policies and procedures if needed
- It is the auditee's responsibility to provide clear, complete, and responsive documentation to OCR
- Entities will not receive "credit" for a later document submission.

If a CE does not have the requested documentation, it must submit an explanation for the deficiency in its response

DESK AUDIT HIPAA CONTROLS

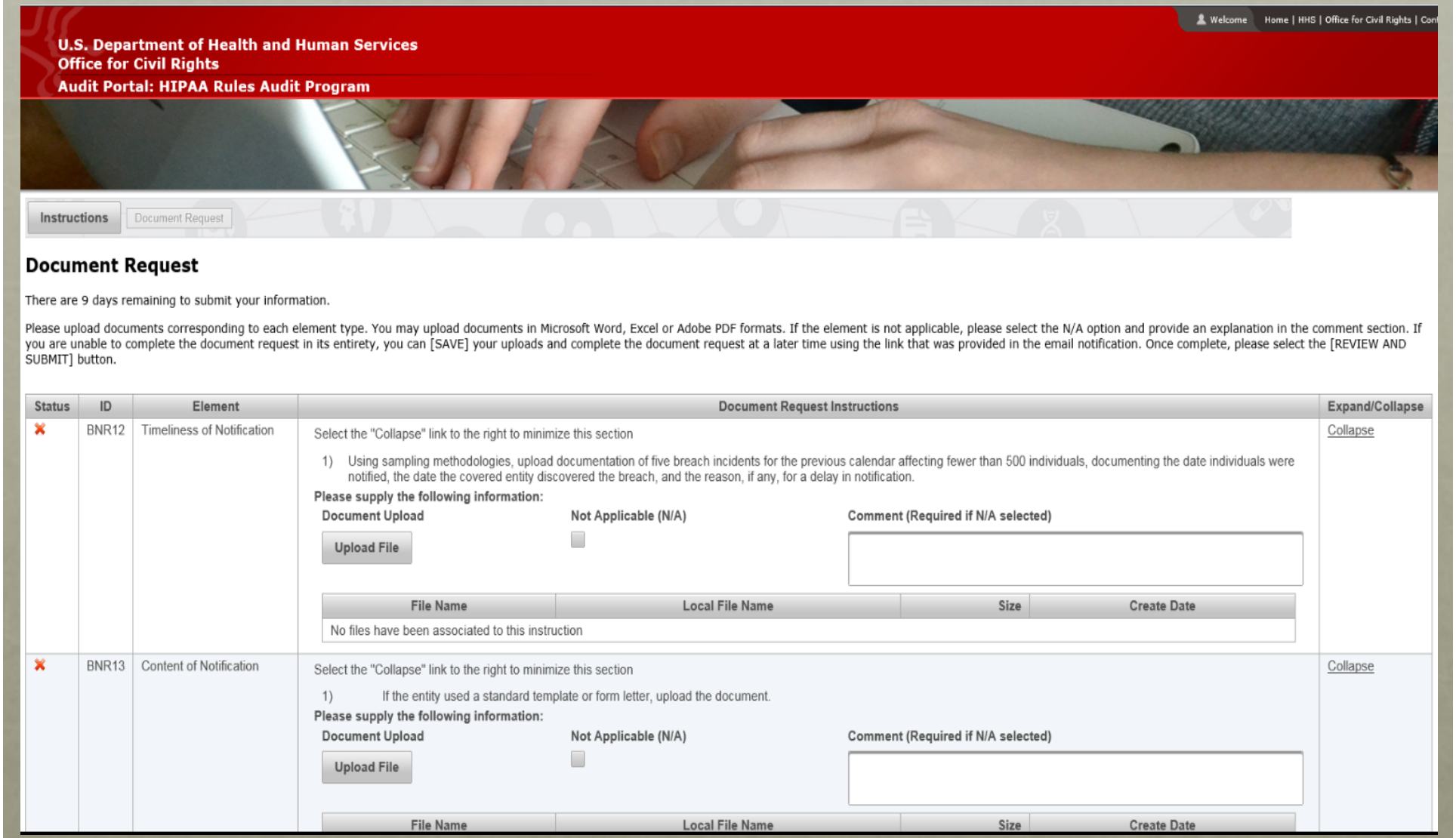
Privacy Rule Controls	Notice of Privacy Practices & Content Requirements [§164.520(a)(1) & (b)(1)]
	Provision of Notice – Electronic Notice [§164.520(c)(3)]
	Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]
Breach Notification Rule Controls	Timeliness of Notification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

DESK AUDIT REPORTING: PROCESS

After review of submitted documentation:

- OCR will develop and share draft findings with the entity
- Entity may respond to draft findings—such written responses will be included in the final audit report
- Final audit reports will describe how the audit was conducted, present any findings, and contain entity responses to the draft findings
- Under OCR's separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit

DOCUMENT REQUEST SCREEN SHOTS



Welcome | Home | HHS | Office for Civil Rights | Cont

U.S. Department of Health and Human Services
Office for Civil Rights
Audit Portal: HIPAA Rules Audit Program

Instructions | Document Request

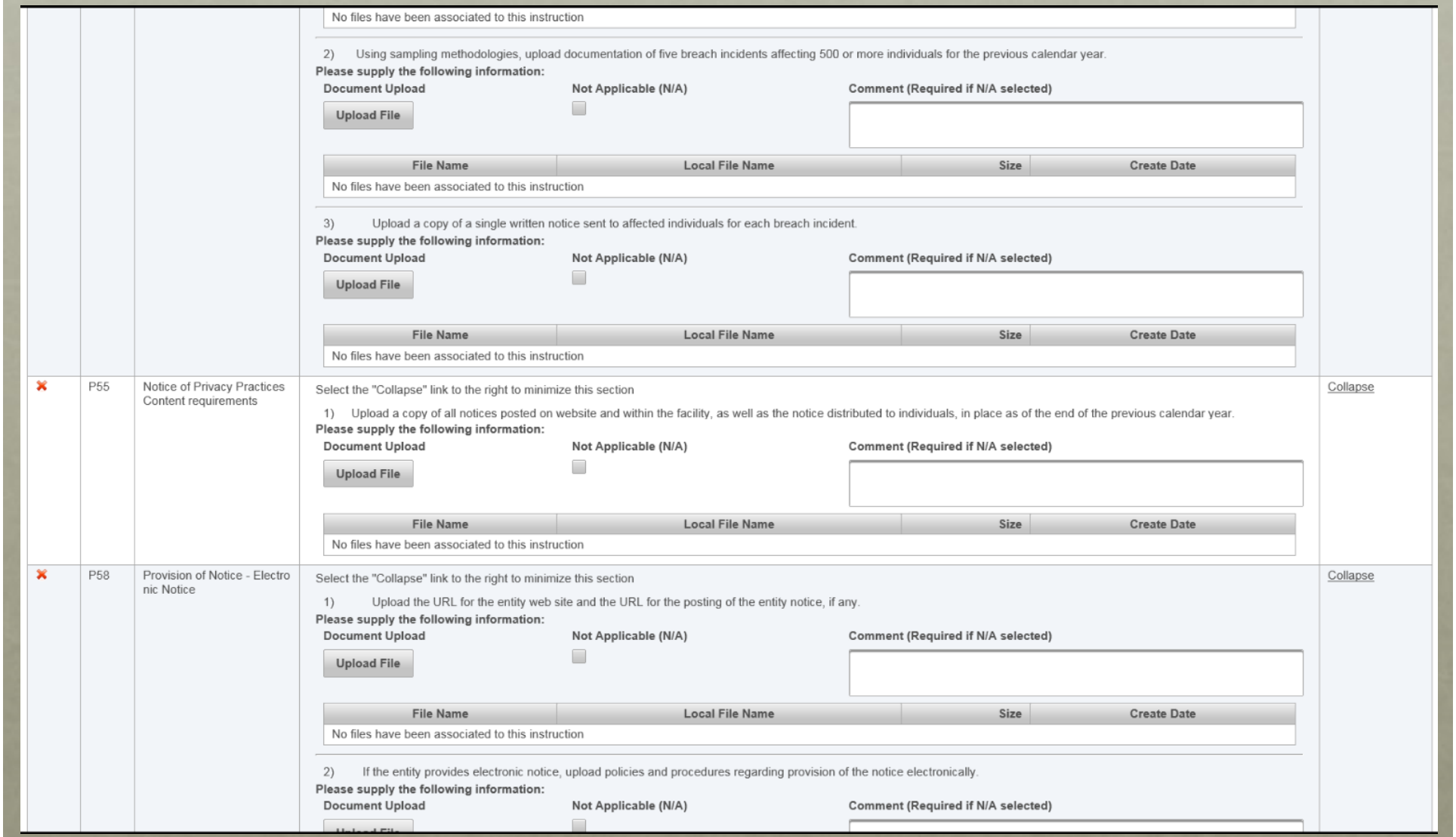
Document Request

There are 9 days remaining to submit your information.

Please upload documents corresponding to each element type. You may upload documents in Microsoft Word, Excel or Adobe PDF formats. If the element is not applicable, please select the N/A option and provide an explanation in the comment section. If you are unable to complete the document request in its entirety, you can [SAVE] your uploads and complete the document request at a later time using the link that was provided in the email notification. Once complete, please select the [REVIEW AND SUBMIT] button.

Status	ID	Element	Document Request Instructions	Expand/Collapse
✘	BNR12	Timeliness of Notification	Select the "Collapse" link to the right to minimize this section 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. **Please supply the following information:** **Document Upload** [Upload File] **Not Applicable (N/A)** ☐ **Comment (Required if N/A selected)** File Name | Local File Name | Size | Create Date No files have been associated to this instruction	Collapse
✘	BNR13	Content of Notification	Select the "Collapse" link to the right to minimize this section 1) If the entity used a standard template or form letter, upload the document. **Please supply the following information:** **Document Upload** [Upload File] **Not Applicable (N/A)** ☐ **Comment (Required if N/A selected)** File Name | Local File Name | Size | Create Date	Collapse

DOCUMENT REQUEST SCREEN SHOTS



No files have been associated to this instruction

2) Using sampling methodologies, upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

3) Upload a copy of a single written notice sent to affected individuals for each breach incident.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

P55 — Notice of Privacy Practices Content requirements

Select the "Collapse" link to the right to minimize this section — Collapse

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.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

P58 — Provision of Notice - Electronic Notice

Select the "Collapse" link to the right to minimize this section — Collapse

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

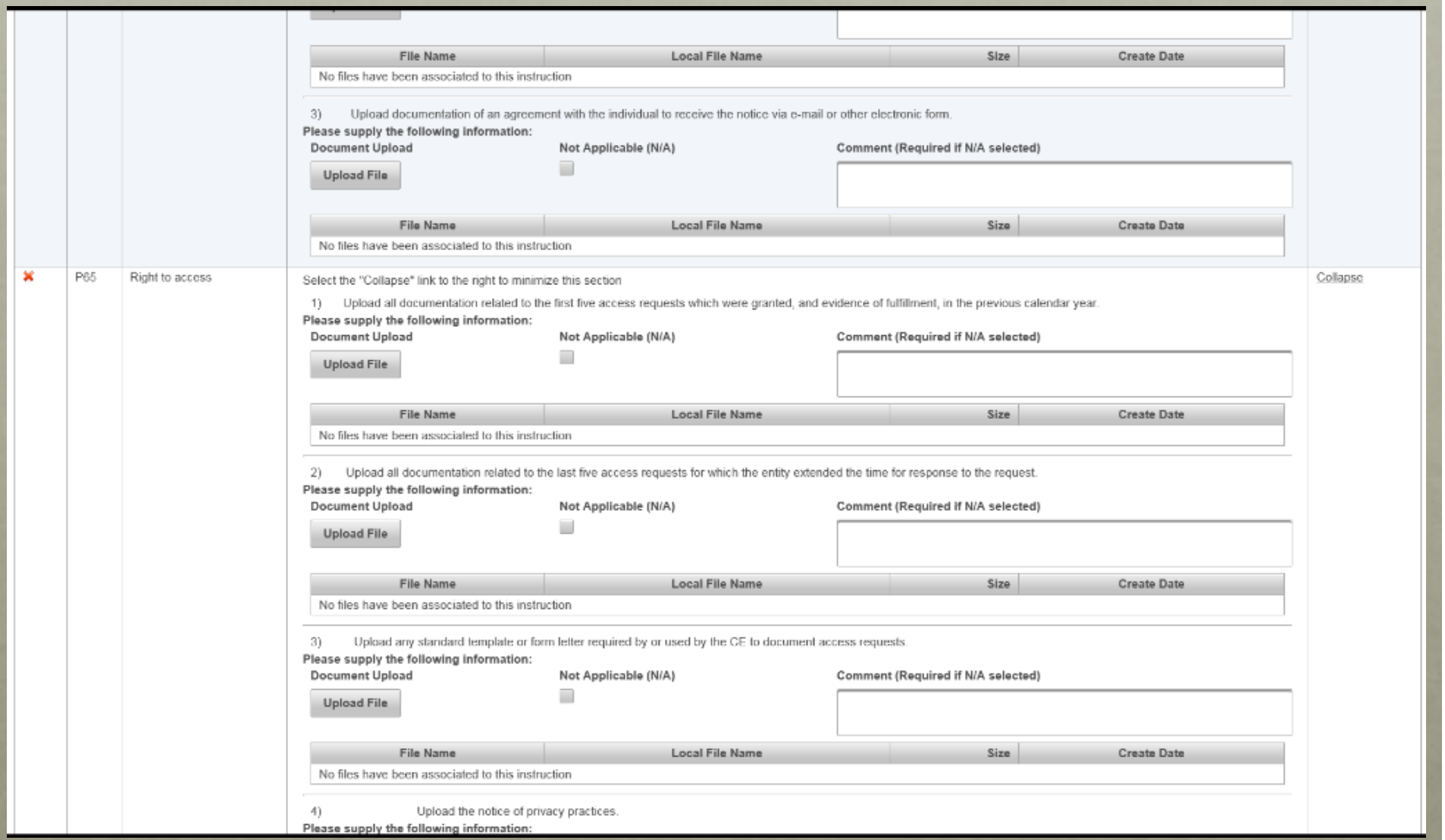
File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

DOCUMENT REQUEST SCREEN SHOTS



			File Name | Local File Name | Size | Create Date No files have been associated to this instruction 3) Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form. **Please supply the following information:** **Document Upload** | **Not Applicable (N/A)** | **Comment (Required if N/A selected)** Upload File File Name | Local File Name | Size | Create Date No files have been associated to this instruction	
✖	P65	Right to access	Select the "Collapse" link to the right to minimize this section 1) Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year. **Please supply the following information:** **Document Upload** | **Not Applicable (N/A)** | **Comment (Required if N/A selected)** Upload File File Name | Local File Name | Size | Create Date No files have been associated to this instruction 2) Upload all documentation related to the last five access requests for which the entity extended the time for response to the request. **Please supply the following information:** **Document Upload** | **Not Applicable (N/A)** | **Comment (Required if N/A selected)** Upload File File Name | Local File Name | Size | Create Date No files have been associated to this instruction 3) Upload any standard template or form letter required by or used by the CE to document access requests. **Please supply the following information:** **Document Upload** | **Not Applicable (N/A)** | **Comment (Required if N/A selected)** Upload File File Name | Local File Name | Size | Create Date No files have been associated to this instruction 4) Upload the notice of privacy practices. **Please supply the following information:**	Collapse

DOCUMENT REQUEST SCREEN SHOTS

DOCUMENT REQUEST SCREEN SHOTS

Status	ID	Element	Document Request Instructions	Expand/Collapse
✖	S2	Security Management Process -- Risk Analysis	Select the "Collapse" link to the right to minimize this section	Collapse

1) Upload documentation of current risk analysis results.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

2) Consistent with 164.316(b)(2)(ii)-(iii), upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to the persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

3) Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

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

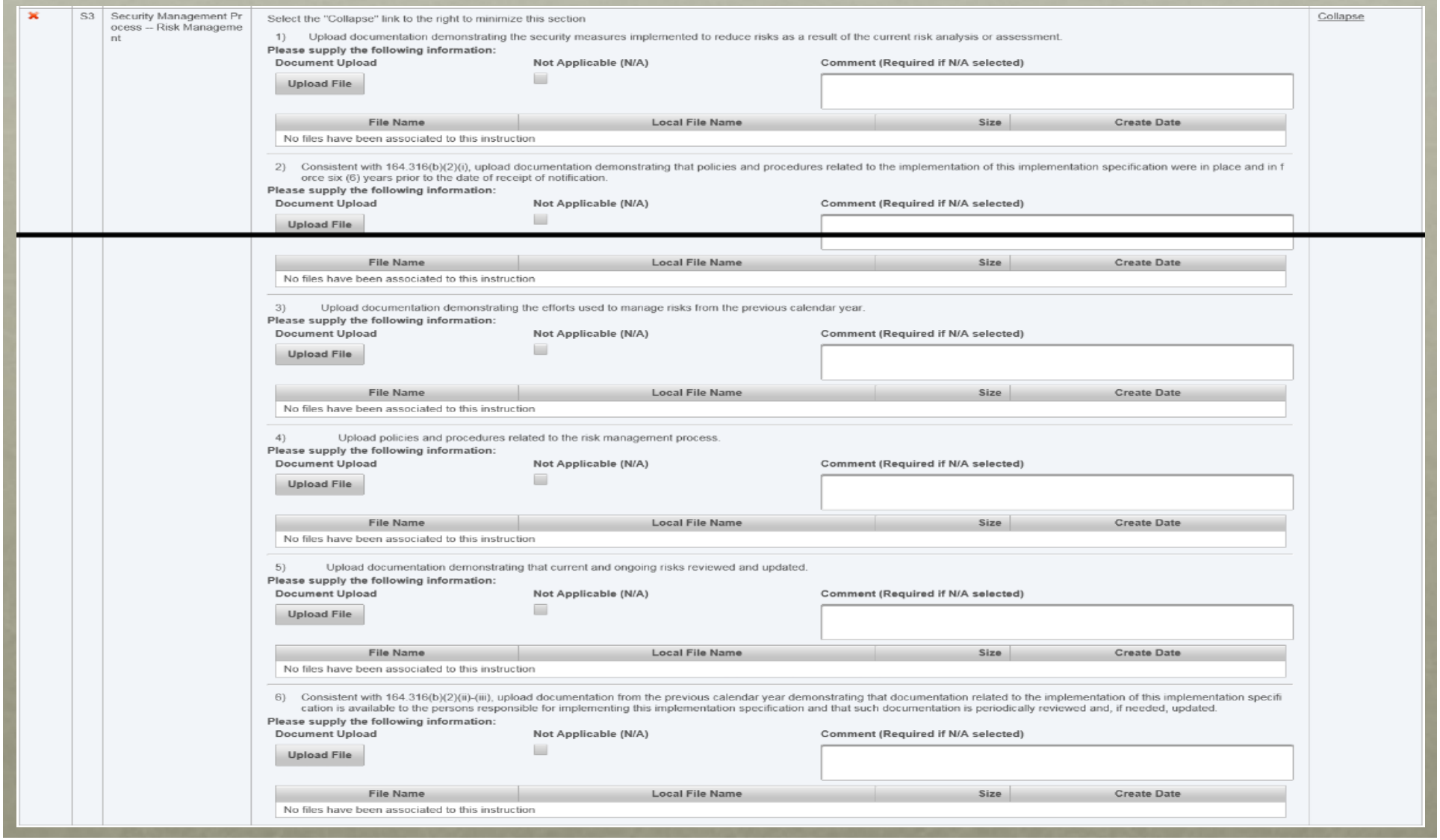
Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

DOCUMENT REQUEST SCREEN SHOTS



S3 | Security Management Process -- Risk Management

Select the "Collapse" link to the right to minimize this section — Collapse

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

2) Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

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

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

6) Consistent with 164.316(b)(2)(ii)-(iii), upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to the persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated.

Please supply the following information:

Document Upload | **Not Applicable (N/A)** | **Comment (Required if N/A selected)**

Upload File

File Name	Local File Name	Size	Create Date
No files have been associated to this instruction			

Q&A SESSION

CONCLUSION & SUMMARY

- Desk Audits are underway!
- OCR will base its audit *only on the documents submitted in the specified electronic process.*
- Business Associates desk audits will commence in the Fall, and the selection pool will be comprised largely of the BAs identified by the CEs in their document responses
- Comprehensive onsite audits of both CEs and BAs will begin in early 2017

ADDITIONAL QUESTIONS?

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

Audit Mailbox: OSOCRAudit@hhs.gov

Zinethia L. Clemmons, Audit Program Manager
Zinethia.Clemmons@hhs.gov
(202) 260-9845

CLOSING REMARKS

Deven McGraw