OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
P55	Privacy	§164.520 (a)(1) & (b)(1)	Notice of Privacy Practices Content requirements	Does the covered entity have a notice of privacy practices? If yes, verify the current notice contains all the required elements. • Header 164.502(a)(1) – Permitted uses and disclosures Does the covered entity include in its notice a description of the following permitted uses and disclosures? • To the individual • For treatment, payment, or health care operations (with at least one example of a use and disclosure for each purpose) • For public health and safety issues • For research purposes • To comply with the law • To respond to organ and tissue donation requests • To work with a medical examiner or funeral director • To address workers' compensation, law enforcement and other government requests • To respond to lawsuits and legal actions. Pursuant to an agreement under, or as otherwise permitted by § 164.510 – Uses and disclosures requiring an opportunity to agree or object: (i) For facility direct (ii) For involvement in the individual's care and notification purposes. 64.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required Does the covered entity include in its notice the following uses and disclosures for which an authorization or opportunity to agree or object is not required: • As required by law • For public health activities • Disclosures about victims of abuse, neglect or domestic violence • For health oversight activities • Disclosures for judicial and administrative proceeding • Disclosures for law enforcement purposes • About decedents • For cadaveric organ, eye or tissue donation purposes • For research purposes • To avert a serious threat to health or safety • For specialized government functions. 164.514 (f)(1) – Standard: Uses and disclosures for fundraising. Required Statements: • A statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization • A statement that the individual may revoke an authorization If the covered entity intends to engage in any of the following activities, separate statements for certain uses or disclosures involving fundraising o A statement that genetic information cannot be used to decide whether coverage can be given or at what price o A statement that information can be disclosed to a plan sponsor for plan administration. Individual rights: Does the notice of privacy practices contain a statement of the individual's rights and a description of how the individual may exercise the following rights:	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.	Q; Do you wish to receive pictures of the Notices hanging on the walls in addition to receiving the uploaded paper copies? A; Yes. Please ensure that the text is readable. Q: Is Request for NPP duplicate? one request under "Right to Access" (subsection 4, and then under "Notice of Privacy Practices" subsection 1 A: Yes, the entity Notice(s) of Privacy Practices is requested in two places within the Privacy section. The documents will be reviewed for overall compliance with the content requirements for Notice in P55.1. In P65.4, the the audit will assess whether the access policies and procedures are congruent with the notice description of the access right. Q: How about NPP translated version. would you like us to submit that as well? A: Yes, provide all versions of the Notice of Privacy Practices

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
				• Obtain a copy of the individual's health and claims records • Request that the covered entity correct health and claims records • Request confidential communications • Ask the covered entity to limit what it uses or shares • Obtain a list of those with whom the covered entity has shared information • Obtain a copy of the privacy notice • File a complaint with the entity and the Secretary of HHS CE Duties: Does the covered entity notify individuals of its legal duties with respect to their PHI, which are: • To maintain the privacy and security of their PHI • To notify affected individual(s) if a breach occurs that compromised the privacy or security of their information • To follow the duties and privacy practices described in the notice • The covered entity will not use or share information other than as described here unless authorized in writing. Authorization may be revoked at any time, in writing. Does the notice state that disclosures will be made: • to the Secretary of HHS for HIPAA rules compliance and enforcement purposes Complaints: The notice must contain a statement that the individual has a right to complain to the CE and to the Secretary if they believe their privacy rights have been violated with a brief description of how to file a complaint with the covered entity and a statement of no retaliation for filing a complaint. Contact: The notice must contain the name or title and telephone number of a person or office to contact for further information. Effective date: The notice must contain an effective date.		
P58	Privacy	§164.520 (c)(3)	Provision of Notice - Electronic Notice	Does a covered entity that maintains a web site prominently post its notice? Does the covered entity implement policies and procedures, if any, to provide the notice electronically consistent with the standard? Determine whether the entity maintains a web site. If so, observe the web site to determine if the notice of privacy practices is prominently displayed and available. An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices. If the covered entity provides electronic notice (such as by linkage to a web page or e-mail), obtain and review the policies and procedures regarding the provision of the notice of privacy practices electronically and the process by which an individual can withdraw their request for receipt of electronic notice. If the covered entity provides the notice of privacy practices by e-mail or other electronic form, obtain and review the documentation of the agreement with the individual to receive the notice via e-mail or other electronic form. Inquire if covered entity has experienced failures when trying to provide the notice of	Upload the URL for the entity web site and the URL for the posting of the entity notice, if any. If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically. Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form.	Q: Can you provide clarity on the electronic request questions in privacy section - is that direct access to the EHR or does providing access to the portal suffice? A: If you review the protocol posted online and examine the document request, you will see that this question pertains to provision of the notice of privacy practices electronically. This question does not involve EHRs.

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
				privacy practices by e-mail. If the covered entity has experienced e-mail transmission failures, obtain and review its attempts to provide a paper copy of the notice via alternative means (e.g., mail).		
P65	Privacy	§164.524 (a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)	Right to access	How does the covered entity enable the access rights of an individual? Inquire of management. Obtain and review policies and procedures in place for individuals to request and obtain access to PHI and to determine whether they comply with the mandated criteria. Determine whether policies and procedures adequately address circumstances in which an access request is made for PHI that is not maintained by the covered entity, per 164.524(d)(3). Obtain and review the notice of privacy practices. Identify whether an individual's right to access in a timely manner is correctly described in the notice. Obtain and review access requests which were granted (and documentation of fulfillment, if any) and access requests which were denied. • Verify that access was provided consistent with the policies and procedures • Verify that requests for access were fulfilled in the form and format requested by the individual if the covered entity can readily produce the PHI in the requested form and format, including electronic format • Determine whether response was made in a timely manner. (e.g., within 30 days of request receipt, unless extension provided consistent with 164.524(b)(2)(ii)) • Determine whether fee charged meets the reasonable cost based fee requirement of 164.524(c)(4) • If the entity denied access to certain PHI, determine whether it provided access to other PHI requested by the individual that was not excluded, per §164.524(d)(1) • For cases for which access was denied, assess whether the denials, and any reviews made pursuant to individual request, were consistent with the policies and procedures. Inquire of management whether the covered entity has used a standard template or form letter for requesting access to protected health information. If the covered entity has used a standard template or form letter for access, obtain and review the document and determine whether it includes the requirements.	Upload policies and procedures for individuals to request access to protected health information (PHI). Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year. (Remove PHI if possible) Upload all documentation related to the last five access requests for which the entity extended the time for response to the request.(Remove PHI if possible) Upload any standard template or form letter required by or used by the CE to document access requests.	Q: On P65 do you want acccess requests from individual only or include access requests from other entities authorized by the individual? A: The individual right to access includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. Therefore requests by the individual to transmit a copy to a designated person should be included. However, requests for disclosures of PHI that are merely authorized by the individual are not considered an exercise of the access right and should not be included. Please see http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs Q; Regarding Access Requests, are you expecting copies of the DRS that we provided to the patient? We believe it should not be included. A: No, audited entities do not need to submit the the DRS provided to the individual in response to an access request. Q; P65 Right to Access- If the access request is from a personal representative on behalf of the patient, are we required to submit documentation proving the personal representative's authority? A: P65 requires all documentation related to the specified access requests. That would include documentation of personal representative status when such status is relevant to the handling of the request. Q; Could you please define "access request?" A: See http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs and http://www.hhs.gov/hipaa/for-professionals/training/index.html Q: In regards to access request, this in regards to just those involved in a breech or all release of information for all including insurances and patients? A: The requests for information about compliance with the access requirements of the Privacy Rule are distinct and separate from the information requests regarding compliance with the Breach Notification Rule. Please review the relevant provisions of the HIPAA rules (see protocol for citations) to help you understand the distinction. Q; Is the right to access about giving the individual information

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
						about who has seen the record? A: See http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html for more information about the the right to access. The individual right to access their protected health information is not the same as their right to request an accounting of disclosures of their information. Q: Regarding the right to access: what documentation is to be uploaded to respond to "all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year." A: There is no one required process for fulfilling access requests under HIPAA and therefore we are not able to specify all the possible documentation. Generally, entities should have a record of the requests they have received and filled in 2015. Do not submit copies of the PHI provided to the individual in response to the individual's request. Q: In a physician office, would access request apply to all requests for medical records by a patient? A: Generally, an individual has a right of access to inspect 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, and the covered entity must permit individuals to request access to that information. Access requests include requests for medical records made by patients that fit this description. See the OCR access guidance http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Q: Is an "access request" the whole record set? What about a request for a single record or just certain payments or just a explaination(s) of benefits (EOB(s))? A: An access request may be for the entire designated record set but is not limited to that. An individual may request access to portions of the record, such as a medication list, a lab report or other information. See the OCR access guidance http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Q: Can you provide an example of what would be "evidence of fulfillment" with respect to right to access (P65). For example, if our access request form includes a section where a workforce member signs off that he or she has completed or responded to the access request and it is signed and dated...would that work? A: Yes, that is an example of "evidence of fulfillment." Other entities may have other types of documentation.

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
S2	Security	§164.308 (a)(1)(ii)(A)	Security Management Process -- Risk Analysis	Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits? Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits? Determine how the entity has implemented the requirements. Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains: • A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis, in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event. If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why.	Upload policies and procedures regarding the entity's risk analysis process. 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. 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. Upload documentation of the current risk analysis and the most recently conducted prior risk analysis. Upload documentation of current risk analysis results.	Q; Can we submit documentation of an annual risk assessment performed by third party? A: Yes, a covered entity may use a business associate to conduct the risk analysis and the results may be submitted in response to S2 (1), Security Rule Risk Analysis. Q; If we recent conducted a risk analysis, but the report is in draft form - should we submit the draft, as well as the prior finalized risk analysis? A: Where entities are asked to provide documentation for a specified time period (e.g., current, previous calendar year, 6 years ago) they should submit documentation that reflects what is in place and in use during the time frame specified. Q: Can you please clarify the difference between S2 question 1 and 5? A: Question 1 is asking for the results of the risk analysis. Question 5 is asking for documentation that the risk analysis was conducted. Q: For the SR S2 Document request, is the request to upload documentation of CURRENT risk analysis results refering to 2015? A: Current means what is in place and in use as of the date of the notification letter you received--July 11, 2016. Q: Can you please be more specific about 6 previous years of risk assessments - that's a lot of documentation? I am only seeing request for 6 previous years of policies - can you repeat again where this request is? A: Question S2.3 and S3.2 both ask for documentation that the subject policies and procedures were in place and in effect 6 years prior to the date of the notification letter--i.e, July 11, 2010. The questions do not require documentation of what was in effect during the intervening years. Q: What would be an example of proof that the risk analysis was available to the workforce members? A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Q: For SR audits, do all the Security Policies and documentation need to be submitted or is there a specific list that you can provide.

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
						A: Refer to the audit protocol for more information about the audit inquiry, which may help you determine what documentation to submit. Q: Do you truly want us to upload our current risk analysis to the portal? This would list vulnerabilities in our system (which we are working to resolve) and they would possibly become public knowledge under the FIOA? A: We believe that a risk analysis submitted by a CE for the audit to be covered by the following exemption from FOIA: Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged. Q: If the most current risk analysis is not that "current", do you recommend having one performed within the time frame allotted and submit this? If so, do you recommend having it done internally, or third party? A: No, do not create a new analysis. Current means as of July 11, 2016, not later. Q: Please explain what you are looking for in S2 Number 2. Are you looking for training records? A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Training records are not responsive to the request. Q: Would the absence of a HIPAA security risk analysis be viewed as a "significant threat" to PHI potentially triggering an enforcement action? A: Please include in the comment field a rationale for why a risk analysis will not be submitted Q: For clarification on Security audit, you listed 164.308 at beginning of slides and then 164.316 in the sample audit -- are you asking for only one area A: 164.316 is the provision that requires covered entities and business associates to implement reasonable and appropriate policies and prcodures to implement the required safeguards (e.g. for 164.308, risk analysis and risk management); to maintain documentation of them for 6 years; and to review that documentation periodically and update as needed.

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
						Q: Our security policies have an effective date as well as a historical record of annual revisions. I assume that will suffice for the six year requirement of what "was" in place? A: Yes Q: Since the questions seem similar in nature, we discerned that the S2 questions were about the documentation of policy/procedures, and S3 is about the "what you actually did" ... is this correct? A: The subject of S2 is risk analysis--the conduct of an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. The subject of S3 is the risk management plan implemented to reduce those identified risks and vulnerabilities to a reasonable and appropriate level. Documentation of the entity's policies and procedures is required as well as documentation showing that the activities required by the policies and procedures have been conducted. Q: If the current risk analysis is 2015, the most recenlty conducted prior risk analysis is 2014? A: Current means what is in place and in use as of the date of the notification letter you received--July 11, 2016. The most recently conducted prior risk analysis would be the one conducted prior to the current one. Q: To validate S2.2, would a simple organization chart of the security organization suffice? Maybe include committee minutes? A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Another example could be committee meeting minutes documenting the efforts the entity has in place to ensure appropriate personnel have appropriate access to the documentation required to implement the procedures of the security rule to which the documentation pertains. To the extent that an organizational chart could assist in the identification of individuals or groups identified in the supporting documentation, such organizational information should also be submitted.

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
S3	Security	§164.308 (a)(1)(ii)(B)	Security Management Process -- Risk Management	Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process. Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.	Upload policies and procedures related to the risk management process. 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. 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. Upload documentation demonstrating the efforts used to manage risks from the previous calendar year. Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment. (Upload documentation demonstrating that current and ongoing risks reviewed and updated.)	Q: Some of the documentation around risk analysis and management seems to apply to several of the different layers of request. Should we upload to each individual question? A: The questions each ask for different documentation; of existing policies and procedures, or evidence that an analysis was conducted or risks addressed, or the results of those actions. Q: What constitutes appropriate documentation for questions that relate to security measures/recommendations being given to and reviewed by appropriate personnel? A: Management approval of plans and/or projects to implement security measures to remediate or mitigate identified risks. Such approvals could take the form of management signatures on risk management plans or other indicators of approval for implementation and/or documentation showing approval and funding of specific projects to implement security measures. Q: Could you provide an example of documentation that would demonstrate people had access to what they needed? This is in the Security section. A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Q: Risk assessments are a daily ongoing process and the technical controls implemented are vast. How much evidence is enough or not enough? We want to make sure we strike the right balance. A: The amount of evidence required to show compliance with the risk analysis implementation specification is whatever amount is necessary to show that an accurate and thorugh assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of all of the ePHI the entity creates, receives, maintains or transmits has been conducted. Q: The security request to provide documentation the the proper people had access to the information is confusing. Can you please clarify what is being request? Are you looking to see that employees of a CE have access to policies? Or are you asking if the authorized individuals in management are reviewing security risk assessments

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
						A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access.

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
BNR12	Breach	§164.404 (b)	Timeliness of Notification	§164.404(b) Timeliness of Notifications Were individuals notified of breaches within the required time period? Inquire of management. [Obtain and review the policies and procedures for notifying individuals of breaches and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach.]--*Not included in current audit* Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).	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.	Q; Under BNR13 Content Notification, you ask for an upload of a written notice sent to affected individuals. If we do not have a breach incident affecting over 500 individuals, should we identify this as not applicable or provide you with a letter from a notice of breach under 500? A: If the entity has not reported a breach involving 500 or more individuals in the specified time period, the entity should search for and provide the evidence from breaches in previous time periods until the requested number of events is reached. If the entity has reported in total fewer than 5 breaches involving 500 or more individuals, the entity may attest to it using the comment field. Q; If we do not have the number of incidents requested and have to go back, do we need to provide the ones that are within the time frame requested in addtion to the ones in the previous time frame not requested? A: Yes. If you do not have documentation of the full number of events in the specified time interval, search back and include additional events in previous time intervals until you are able to compile the specified number. If you have not experienced the total number of requested events, be sure to attest to that in your submission. Q: BNR12: Can we enter this information into an Excel spreadsheet? Or do you need the documentation for each data element? A: A spreadsheet would be helpful, but all the specific documentation requests must be met--which likely will require additional documentation. Q: we had a incident in December but once the audit was concluded we reported in January 2016. can we count that for 2015? A: You may reach your own determination of what to include in documentation "for the previous calendar year" (i.e., 2015).

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
BNR13	Breach	§164.404 (c)(1)	Content of Notification	§164.404(c)(1) Content of Notification Evaluate if the specifications at §164.404(c) are met. Inquire of management whether the covered entity has used a standard template or form letter for notification to individuals for all breaches or for specific types of breaches. If the covered entity has used a standard template or form letter for breach notification, obtain and review the document. Evaluate whether it includes this section's required elements. Obtain and review a list of breaches, if any, in the specified period and documentation of written notices sent to affected individuals for each breach. Select notifications sent to individuals to be reviewed and verify that the notices include the elements required by §164.404(c). [Does the covered entity have policies and procedures for providing individuals with notifications that meet the content requirements of §164.404(c)? Inquire of management; obtain and review policies and procedures.] Not included in current audit	Upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year. Upload a copy of a single written notice sent to affected individuals for each breach incident. If the entity used a standard template or form letter, upload the document.	Q: In BNR 12 and 13, can you provide an example or elaborate on appropriate "sampling methodologies"? A: You may ignore the phrase "using sampling methodologies." This phrase will be deleted from the document submission pages. Q; For BNR #3 are you requesting all breach letters sent in the previous year or just one letter sent as an example? A: BNR13.3 asks for a single copy of the notification sent to individuals for each event. So if you have experienced three breaches, provide one letter for each breach. Q: We had five HIPAA incidents (assumed breaches) in 2015. However, if we determined after an analysis that notification was not required for all breaches in 2015, would you like us to provide a notification from 2014? A: We are asking for documentation for breaches for which notification was provided. If you did not have a sufficient number for 2015 to meet the request, please add incidents from previous years until you reach 5 total. Q: BNR13 -3 copy of single written notice-is this for 500< only? A: BNR13.3 asks for a single copy of the notification sent to individuals for each breach event, regardless of size. So if you have experienced one breach under 500 and two over 500, these count as three breach events, and you would provide one letter for each. Q: we are small pharmacy and only sent out one breach notification to a patient …should we just upload that one ? A: If you only have a total of one breach notification, attest to that in the comment box and provide the required documentation for that one notification. Q: Breach definition: would that include all the unpermitted/unintended releases that were not reported? How about cases that were only reported to States? A: The subject of this section is breach notification. Please provide information regarding breaches for which you determined notification was required by the HIPAA Breach Notification Rule. State law reporting is not the subject of this audit. Q: We are an entity with one tax ID, and many sites. One of our sites was identified for the audit, and we report the HIPAA breaches as an entity. We have only had one breach for that particular site that was identified. Do I just enter that one breach? SHould I use all sites as response for the breach examples? A: Use your best judgement. In general, notifications were sent to the location of interest. If the address was to a headquarters, reply based on the entire entity.