OCR Desk Audit Criteria (July 2016)

S2 Security Management Process Risk Analysis

1. Upload documentation of current risk analysis results.
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
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.
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.

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. 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.
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. 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

Note: *In public presentations at conferences, the OCR has repeatedly emphasized the need for encryption. They have been quoted as saying, "Encrypt everything!" Therefore, a risk management plan should include encryption; in particular, end point devices: portable media, laptops/tablets, smartphones, and high-risk workstations, etc.*

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.

P55 NPP 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, 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 email or other electronic form.

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

For all documentation: Policies, procedures, plans, etc. – reviewed, updated, and approved

§ 164.316 Policies and procedures and documentation requirements

- **(i) Time limit** – Retain the documentation for 6 years
- **(ii) Availability** – Make documentation available to the workforce
- **(iii) Updates** – Periodically review, update, and approve

Inventory of all Business Associates/w contact information (building a database of BAs)
(See additional attachment – "Phase 2 Audits and Request for Business Associate Listing")

How does the covered entity "… attempts in good faith to obtain satisfactory assurances [from business associates] as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained." [ref: HIPAA Security Rule]