2016-2017 HIPAA AUDITS INDUSTRY REPORT

Department of Health and Human Services
Office for Civil Rights
Health Information Privacy Division
December 2020

TABLE OF CONTENTS

Figures

SUMMARY

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) requires HHS to periodically audit covered entities and business associates for their compliance with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)/HITECH Privacy, Security, and Breach Notification Rules (HIPAA Rules).[1] In 2016 and 2017, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) conducted audits of 166 covered entities and 41 business associates regarding compliance with selected provisions of the HIPAA Rules. Based on its findings, OCR concluded that most covered entities met the timeliness requirements for providing breach notification to individuals, and most covered entities (that maintained a website about their customer services or benefits) also satisfied the requirement to prominently post their Notice of Privacy Practices (NPP) on their website. However, OCR also found that most covered entities failed to meet the requirements for other selected provisions in the audit, such as adequately safeguarding protected health information (PHI), ensuring the individual right of access, and providing appropriate content in their NPP. OCR also found that most covered entities and business associates failed to implement the HIPAA Security Rule requirements for risk analysis and risk management.

HHS offers many tools to assist entities in complying with HIPAA. For example, entities can consult the recently updated HHS Security Risk Assessment Tool and OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule for help in evaluating whether they have a compliant risk analysis and risk management process. An entity can use one of OCR's model notices of privacy practices, as a template, to ensure it includes all of the HIPAA required statements in its NPP. Additionally, OCR's access guidance clarifies how covered entities can improve patients' access to their health information by implementing improved policies and procedures and digital technologies. This report includes links to HHS guidance and other resources offered to covered entities and business associates to improve their compliance with the HIPAA Rules.

INTRODUCTION

OCR administers and enforces the HIPAA Rules (45 CFR Part 160 and Part 164 Subparts A, C, D and E), which establish requirements with respect to the use, disclosure, and protection of PHI by covered entities and business associates; provide health information privacy and security protections; and establish rights for individuals with respect to their PHI. The Privacy and Security Rules were promulgated pursuant to the administrative simplification provisions of HIPAA, and amended in accordance with, and pursuant to, HITECH and the Genetic Information Nondiscrimination Act of 2008 (GINA). HHS also promulgated the Breach Notification Rule pursuant to HITECH, which requires a HIPAA covered entity to notify

[1] HITECH was enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), Section 13411 of HITECH, which became effective on February 17, 2010, authorizes and requires the Department to undertake periodic audits to ensure that covered entities and business associates comply with the HIPAA Rules.

affected individuals, HHS, and in some cases the media--and requires a business associate to notify its covered entity--following a breach of unsecured PHI.

Section 13411 of HITECH requires HHS to audit covered entity and business associate compliance with the HIPAA Rules: "The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements."[2]

This report describes the audits conducted during 2016 and 2017, the results, and recommended technical assistance for covered entities and business associates regarding the deficiencies identified.

PURPOSE

The audits gave OCR an opportunity to examine mechanisms for compliance, identify promising practices for protecting the privacy and security of health information, and discover risks and vulnerabilities that may not have been revealed by OCR's enforcement activities. These audits were designed to complement OCR's enforcement program, which investigates specific covered entities or business associates through complaint investigations and compliance reviews; seeks resolution of potential violations through corrective action plans and settlements; and, in some instances, imposes civil money penalties. OCR's audits will enhance industry awareness of compliance obligations and enable OCR to better target technical assistance regarding problems identified through the audits. Through the information gleaned from the audits, OCR has developed, and will continue to develop, tools and guidance to assist the industry in compliance, self-evaluation, and preventing breaches.

AUDIT PROCESS

OCR's Phase 1 audits (Audit Pilot Program), conducted in 2012, included comprehensive on-site audits of covered entities' documentation and implementation of the HIPAA Rules. For Phase 2, between 2016 and 2017, OCR focused on testing the utility and cost effectiveness of desk audits of HIPAA covered entities' and business associates' (together, entities) compliance with selected provisions of the HIPAA Rules.[3]

OCR developed a comprehensive audit protocol for use in the desk audits to analyze an entity's compliance with the processes, controls, and policies relating to the HIPAA Privacy, Security, and Breach Notification Rules. The audit protocol addresses every standard and implementation specification of these Rules and provides measurable criteria and key questions an entity can apply when developing and reviewing its compliance activities. The audit protocol is organized by Rule and regulatory provision and addresses separately the requirements for (P) privacy, (S) security, and (BNR) breach notification. The protocol is further organized by numbered elements, which contain audit analysis requirements for one or more standards of the Rules. For

[2] *See* 42 U.S.C. § 17940.

[3] In this report, the terms *covered entities* or *business associates* are used when presenting information about one or the other type of entity*; entities* is used when referring to both covered entities and business associates.

example, element P55 contains audit criteria for the NPP content requirements. Each element contains the regulatory sections to be addressed, describes a key activity and established performance criteria, the audit inquiry to be made, and the documents that will be reviewed. The audits performed assessed entity compliance with selected requirements and varied based on the type of covered entity or business associate selected for review. The protocol is available on OCR's website as a tool that entities can use to gauge, and better understand, their own compliance.

Entities that were selected for a Phase 2 audit received two email communications: an initial notification letter and a document request. The notification letter provided instructions for responding to the document request, the timeline for response, and a unique link for each entity to submit documents via OCR's secure online portal. In addition to the document request, the second email also provided information about an opening meeting with OCR to discuss the audit, as well as an additional request for covered entities to provide a list of their business associates.[4] Further information about entity selection and audit program management is available on the OCR audit webpage.

Entities were given 10 business days to respond to the document requests. The specific documents OCR requested are described in the Audit Results section. In performing the audits, OCR reviewed, against the audit protocol, the policies, procedures, and other requested documentation that each entity submitted.

After completing its initial analysis of the submitted materials, OCR provided draft findings to the entities and gave them an opportunity to respond with comments or descriptions of any completed or planned corrective actions. OCR considered the entity's responses when preparing the entity's final report. Each final report incorporated comments and descriptions of any corrective actions that were submitted by the entity and OCR's assessment of those comments, when appropriate.

ENTITY SELECTION

For Phase 2 audits, OCR identified pools of covered entities that represent a wide range of health care providers, health plans, and health care clearinghouses to better assess HIPAA compliance across the industry. To ensure a broad cross-section of covered entities, OCR's sampling criteria included size, affiliations, location, and whether an entity was public or private. Health plans were divided into group plans and issuers and providers were further categorized by type of hospital, practitioner, elder care/skilled nursing facility (SNF), health system, or pharmacy. OCR then ran a randomized selection algorithm that drew from each of the categories to produce a pool of covered entities. Finally, the auditees were checked for conflict of interests with the contractor supporting OCR in the audit process, as well as whether they were the subjects of open OCR investigations or compliance reviews. The 166 audited covered entities submitted lists of all their business associates, which OCR combined to create a pool of business associates. OCR chose 41 business associates through a randomized selection from this pool.

[4] Desk audits of business associates followed in 2017 after the completion of the covered entity desk audits.

NUMBERS AND TYPES OF COVERED ENTITIES

The vast majority of audited covered entities were health care providers (150 of the 166 total). See Figure 1. A wide range of health care providers were represented including practitioners, pharmacies, hospitals, health systems, skilled nursing facilities, and elder care facilities. See Figure 2.

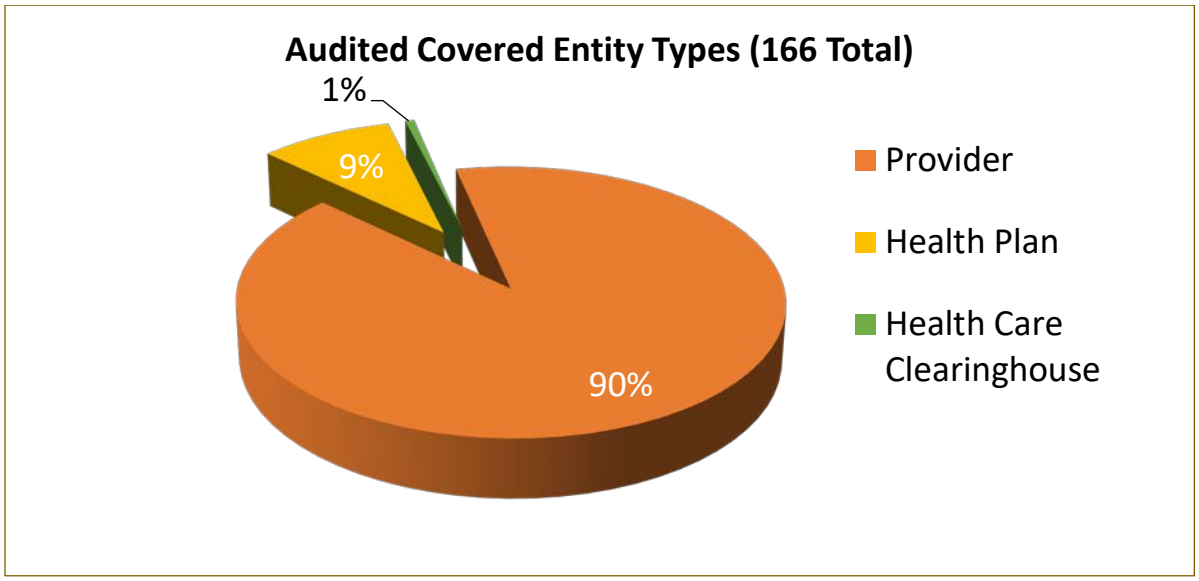

FIGURE 1 AUDITED COVERED ENTITIES, PERCENTAGE OF 166 BY TYPE

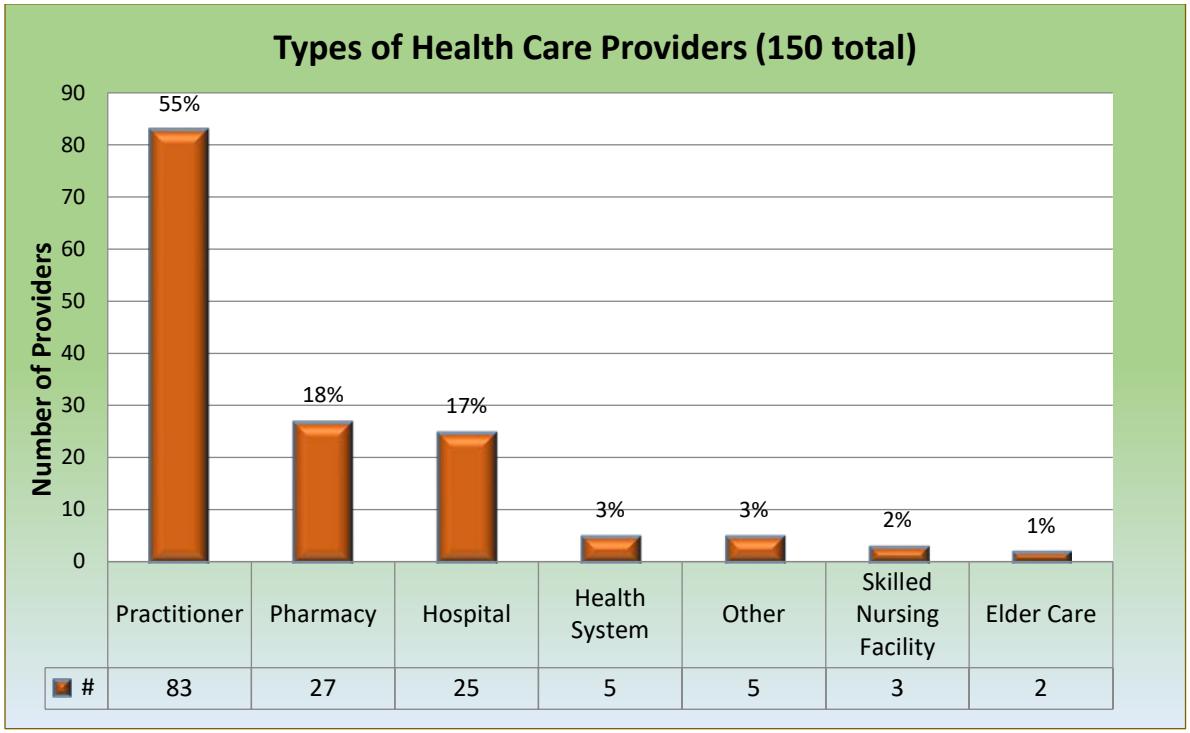

FIGURE 2 TYPES OF HEALTH CARE PROVIDERS

COVERED ENTITY – AUDITED HIPAA RULES PROVISIONS

The provisions of the HIPAA Rules selected for the Phase 2 audits of covered entities were based on the results from the 2012 audits and recent OCR enforcement activities, which identified weakness in entity implementation in certain areas. For example:

- The audits conducted in 2012 identified problems in security risk analysis and risk management, consistent with OCR's findings in investigations and enforcement actions. The identification of potential risks to, and vulnerabilities of, electronic protected health information (ePHI), and the implementation of security measures to reduce those risks and vulnerabilities are requirements of the HIPAA Security Rule.
- The HIPAA Privacy Rule established an individual's right to access, inspect, and obtain a copy of their PHI in a designated record set upon request to a covered entity. An individual has the right to receive the information electronically and in their preferred form and format, if the entity has the ability to readily produce it. See 45 CFR § 164.524.

Covered entities were audited either on the selected provisions of the Privacy and Breach Notification Rules, or the Security Rule provisions. Covered entities were asked to submit documentation of their compliance with the requirements listed in Figure 3. Based on a random assignment of the 166 covered entities audited, 103 were audited on the privacy and breach provisions and 63 were audited on security requirements.

HIPAA RULE	PROVISIONS EXAMINED IN COVERED ENTITY AUDIT
Privacy Rule	**Notice of Privacy Practices & Content Requirements** §§ 164.520(a)(1) & (b)(1)
	Provision of Notice – Electronic Notice (Website Posting) § 164.520(c)(3)(i)
	Right of Access §§ 164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)
Breach Notification Rule	**Timeliness of Notification** § 164.404(b)
	Content of Notification § 164.404(c)(1)
Security Rule	**Security Management Process -- Risk Analysis** § 164.308(a)(1)(ii)(A)
	Security Management Process -- Risk Management § 164.308(a)(1)(ii)(B)

FIGURE 3 COVERED ENTITY AUDITED PROVISIONS

NUMBER AND TYPES OF BUSINESS ASSOCIATES AND AUDITED PROVISIONS

Selected covered entities were asked to identify and provide detailed information regarding their business associates. The information collected was used to help identify business associates for the Phase 2 audits.

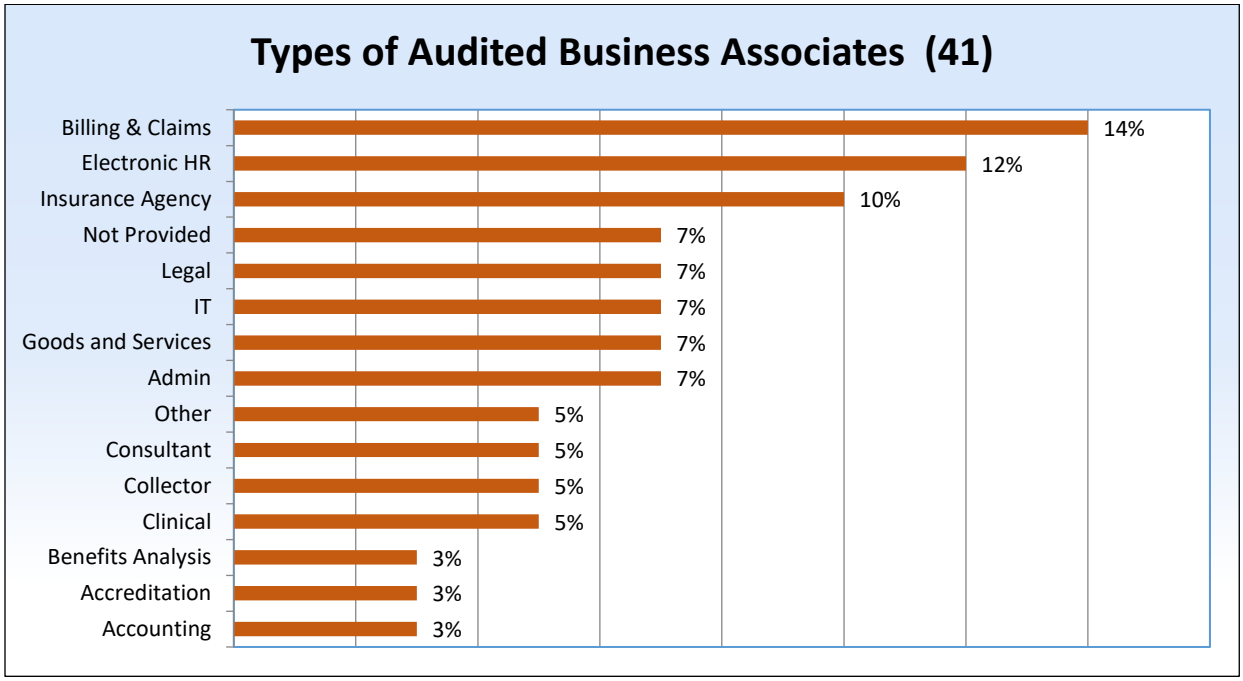

FIGURE 4 TYPES OF BUSINESS ASSOCIATES

Each of the 41 business associates were audited on the breach and security requirements listed below, in Figure 5.

HIPAA RULE	PROVISIONS EXAMINED IN BUSINESS ASSOCIATE AUDIT
Breach Notification Rule	**Notification by a Business Associate** § 164.410, with reference to Content of Notification § 164.404(c)(1)
Security Rule	**Security Management Process -- Risk Analysis** § 164.308(a)(1)(ii)(A)
	Security Management Process -- Risk Management § 164.308(a)(1)(ii)(B)

FIGURE 5 BUSINESS ASSOCIATE AUDITED PROVISIONS

RATINGS

The entity-specific final reports explained OCR's analysis and rating of each entity's compliance efforts for every audited element on a scale of 1 to 5. The scores identified OCR's assessment of the comprehensiveness and effectiveness of entity activities. A rating of 1 reflects a high understanding and strong implementation of the audited elements. A 2 rating reflects activities that are largely in compliance, but reveal some weaknesses. A 3 or 4 rating reflects serious shortcomings in compliance efforts, and a 5 means no serious effort was taken by the entity. See Figure 6, *Audit Compliance Effort Ratings – Legend*, below, for more information.

Audit Compliance Effort Ratings—Legend

Rating	Description
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	The audit results indicate the entity's efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - *e.g.*, policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of a serious attempt to comply with the Rules.

FIGURE 6 COMPLIANCE EFFORT RATING LEGEND

AUDIT RESULTS

Figures 7 and 8 summarize the ratings assessed to covered entity and business associate compliance efforts related to the assessed protocol elements. The blue and red colors correspond to the most frequent ratings applied by OCR for each element reviewed. Blue applies to a 1 or 2

rating, identifying positive outcomes and appropriate compliance activities. Red identifies implementation as inadequate, negligible, or absent. The entity would need to take remedial action to ensure appropriate privacy or security safeguards are in place for PHI, and individual access requests can be met. At a glance it is clear that the subjects of the audits largely failed to successfully implement these HIPAA Rules requirements.

Generally, covered entities demonstrated compliance in two of the seven areas audited: (1) timeliness of breach notification (BN) and (2) prominent posting of NPP on their websites. As discussed below, covered entities generally attempted to comply with the individual access and content of breach notification provisions, but 89% (access) and 67% (notification content) failed to document adequate compliance. Consistent with the findings of the Phase 1 audits, covered entities still struggle to implement the Security Rule's requirements of risk analysis and risk management. Most reviews produced ratings in the 3-5 range.

Covered Entity Audited Provisions		Rating					
Protocol Element #	Provision	1	2	3	4	5	N/A
P55	NPP	2	**34**	**40**	11	16	0
P58	Electronic Posting of NPP	**59**	**16**	4	6	15	3
P65	Access	1	10	**27**	**54**	11	0
BNR12	BN Timeliness	**67**	6	2	9	**12**	7
BNR13	BN Content	14	15	**24**	**38**	7	5
S2	Risk Analysis	0	9	**20**	**21**	13	0
S3	Risk Management	2	2	15	**28**	**16**	0

FIGURE 7 COVERED ENTITY RATINGS

Business associates achieved audit ratings similar to those achieved by covered entities in security risk analysis and risk management. Most of the audited business associates (32 of 41) reported not having experienced any breaches of unsecured PHI. The audit results of business associates that had experienced a breach primarily identified minimal (3 rating) or negligible (4 rating) efforts to address audited requirements.

Business Associate Audited Provisions		Rating					
Protocol Element #	Provision	1	2	3	4	5	N/A
BNR17	Notice to Covered Entities	0	2	**4**	**3**	0	**32**
S2	Risk Analysis	3	4	**16**	**12**	6	0
S3	Risk Management	0	5	**8**	**21**	7	0

FIGURE 8 BUSINESS ASSOCIATE RATINGS

RESULTS REPORTED BY AUDITED ELEMENT

The following sections contain findings and discussions of how audited entities fared overall within each audited element of the protocols. Element-specific results are organized using the following categories.

- **AUDIT REQUIREMENTS:** The requirements of the subject provisions in the HIPAA Rules.
- **AUDIT RESULTS:** A summary of the findings across audited entities.
- **ENTITY RESPONSE:** Draft findings were provided to the entities along with an opportunity to respond with comments or descriptions of any completed or planned corrective actions. In these sections, OCR summarizes information from the written responses that the audited entities submitted to OCR.
- **POSITIVE OUTCOMES:** This section discusses corrective or other actions taken by audited entities that improved implemented protections for PHI.
- **OPPORTUNITIES FOR IMPROVEMENT:** Observations of areas for continued attention.

ELEMENT – NOTICE OF PRIVACY PRACTICES (P55)

AUDIT REQUIREMENTS:

The HIPAA Privacy Rule requires health plans and covered health care providers to develop and distribute a notice that provides a plain language explanation of individuals' rights with respect to their PHI and the particular privacy practices of the specific health plan or health care provider offering the NPP. 45 CFR §§ 164.520(a)(1) & (b)(1).

DOCUMENTS REQUESTED:

- Copy of NPP distributed to individuals.
- Copy of all NPPs posted on entity website and within the facility.

AUDIT RESULTS:

Element P55, regarding required content of the NPP, revealed widespread failure to provide individuals with the information required. Only 2% of covered entities fully met the requirements, while two-thirds failed to or made minimal or negligible efforts to comply. While most covered entities submitted an NPP that contained certain required statements and elements, such as a header and descriptions of permitted uses and disclosures, the majority of covered entities that received a 3 to 5 rating produced NPPs that lack many required elements. Many entities did not meet the requirement to *provide a notice that is written in plain language.*

Almost all NPPs were missing required content, often related to individual rights. OCR encourages covered entities to either review the model NPP available on the OCR website or refer to the audit inquiry language in the protocol and the requirements set forth in 45 CFR § 164.520 as a reference to the content that must be included for a compliant NPP. Common omissions found during the audits relate to the following content requirements:

- § 164.520(b)(ii)(B) "A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization."
- § 164.520(b)(ii)(D) "the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law."
- § 164.520(b)(iv) "Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information *and a brief description of how the individual may exercise these rights* (emphasis added), as follows:… (C) The right to inspect and copy protected health information as provided by § 164.524."
- § 164.520(b)(ii)(E) "A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5)."

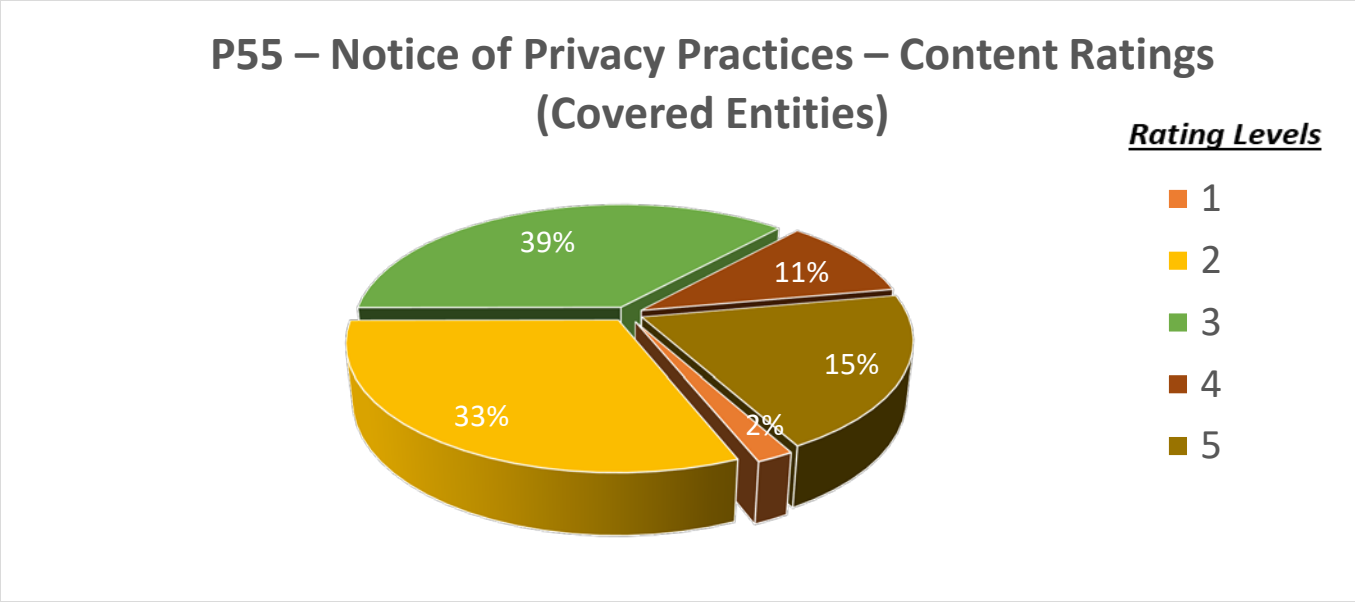

FIGURE 9 NOTICE OF PRIVACY PRACTICES – CONTENT RATINGS

ENTITY RESPONSE: Sixty-seven covered entities audited on this element responded to the draft report; 45 agreed or adopted the recommendations; 12 stated they had misinterpreted the law when conducting their compliance activities or misunderstood the document requirements.

POSITIVE OUTCOMES: A large majority of the covered entities noted their appreciation for the comments or findings, and initiated actions to strengthen policies, procedures, and/or correct deficiencies.

OPPORTUNITIES FOR IMPROVEMENT: Many covered entities failed to meet the content requirements of the NPP standard. However, an easy-to-use resource that covered entities may choose to utilize in preparing their NPPs are the Model Notices of Privacy Practices available on OCR's website. The models include the regulatory changes of the Omnibus Rule (2013). In particular, the models highlight the patient right to access their ePHI held in an electronic health record. Covered entities may customize these models by entering their entity-specific information.

ELEMENT – ELECTRONIC NOTICE, PROVISION OF NOTICE (P58)

AUDIT REQUIREMENTS:

If a covered entity maintains a website that provides information about the covered entity's customer services or benefits, the covered entity must prominently post its NPP and make it available electronically through its website. Audit element P58 examined whether covered entities with consumer websites prominently posted their NPPs and made them available electronically through their website. See 45 CFR § 164.520(c)(3).

DOCUMENTS REQUESTED:

- Electronic NPP policy and procedures.
- URL for the entity website and the URL for the posting of the entity NPP, if any.

AUDIT RESULTS:

The majority, 57%, of audited covered entities received a 1 rating, revealing that they provided documentation that fully satisfied the requirement. These covered entities posted the NPP at a prominent location on their websites, such as through a drop down menu on a home page or on the top or bottom of their home page as a designated link. Three entities did not maintain a website and therefore were not subject to these audited requirements.

Most covered entities that received a lower rating received it in part for their failure to meet the *prominently posted* requirement. Covered entities received a lower rating when they posted their NPP in a non-prominent manner, such as on a page neither directly on, nor accessible from, the homepage. The difference in rating reflects the degree of difficulty in finding the NPP. Examples of insufficient postings include:

- Requiring a user to navigate from the home page to a *Privacy Policy* page and then select *Patient Privacy Notice* on another navigation menu.
- Requiring a user to select the "About Us" page from the homepage.
- Posting links that are labelled as *policy*, *HIPAA*, or *insurance*. As noted in the audit protocol, "an example of prominent posting of the notice would include a direct link from the homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices."
- Maintaining two links with the same title (for example, *privacy policy*) on their homepages, connecting to two different privacy guidelines, one of which was the NPP.

Some covered entities posted NPPs that appeared to be provided on behalf of a different covered entity or other person. The audited covered entity did not describe its relationship with the persons identified on the notice and/or the person described by the website. An individual has a right to adequate notice of the uses and disclosures that may be made by each particular covered entity, their rights, and the covered entity's legal duties. If the linked notice does not identify the covered entity that maintains the website, *adequate notice* has not been provided. Separate covered entities that participate in an organized health care arrangement may use a joint notice that must describe with reasonable specificity the covered entities, or class of covered entities, to which the joint notice applies, as well as the service delivery sites to which the notice applies. See 45 CFR § 164.520(d).

OCR provided a 4 or 5 rating to covered entities for maintaining non-functioning links to their NPP on their websites. These covered entities provided OCR with links to their NPPs that prompted error messages. Each covered entity should ensure its web presence is functional and responsive to consumers' needs.

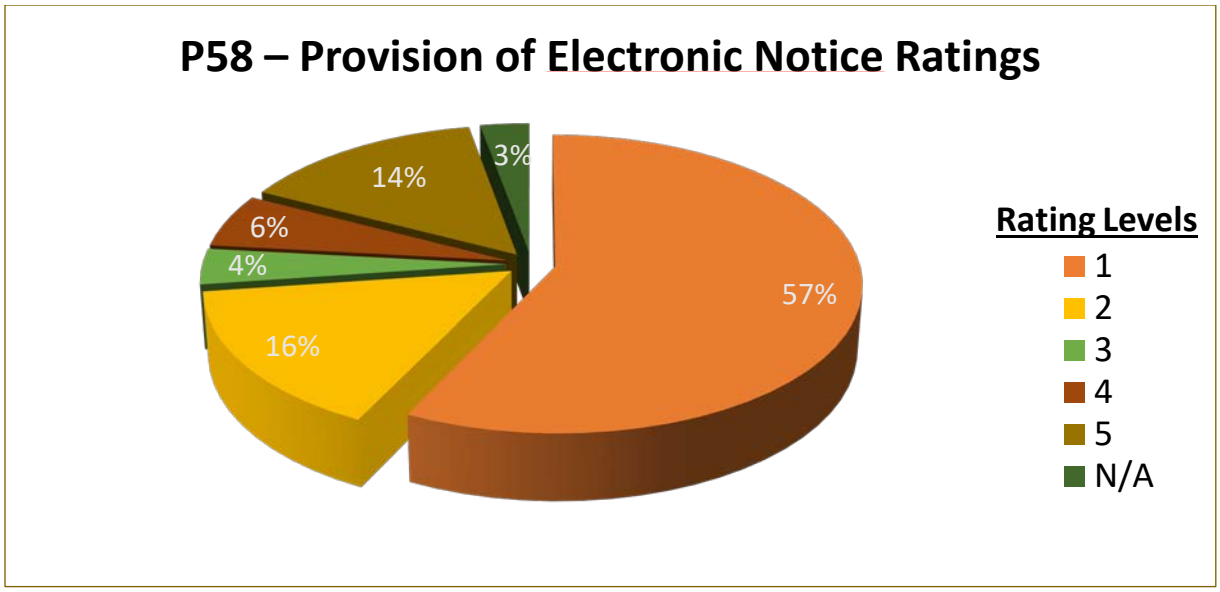

FIGURE 10 PROVISION OF ELECTRONIC NOTICE RATINGS

ENTITY RESPONSE: Thirty-seven covered entities audited on this element responded to the draft report; 29 agreed or adopted the recommendations; one stated it had misinterpreted the law when conducting its compliance activities.

POSITIVE OUTCOMES: Covered entities generally were receptive and responsive to feedback they obtained through the audit of this element.

OPPORTUNITIES FOR IMPROVEMENT: A covered entity should review its web site and consider whether the NPP is prominently displayed, so an individual can find it.

ELEMENT – RIGHT OF ACCESS (P65)

AUDIT REQUIREMENTS:

The Privacy Rule generally requires HIPAA covered entities to provide individuals, upon request, with access to the PHI about them in one or more "designated record sets" maintained by or for the covered entity. This includes the individuals' rights to inspect or obtain a copy, or both, of the PHI; to receive the copy in the form and format requested by the individual, if readily producible in that form and format, or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual; and to direct the covered entity to transmit an electronic copy of PHI in an electronic health record to a person or entity designated by the individual.[5] Individuals have a right to access this PHI for as long as the information is maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (*e.g.*,

[5] In *Ciox Health, LLC v. Azar, et al.*, 435 F. Supp. 3d 30 (D.D.C. 2020), a federal court held that the individual's right to direct PHI to a third party is limited to *an electronic copy of PHI in an electronic health record.* The court also held that the reasonable, cost-based fee limitation does not apply when directing PHI to a third party.

whether by the covered entity, another provider, the patient, etc.).

Covered entities must implement policies and procedures to enable these rights. OCR examined these documented policies and procedures, as well as documentation of their responses to requests for access from their patients and plan members. While the Privacy Rule does not require covered entities to develop and use standard access request forms, they are often used. When they were provided, OCR offered technical assistance on their content. See 45 CFR §§ 164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3).

DOCUMENTS REQUESTED:

- Access requests.
- Extensions to access requests.
- Access requests templates and/or forms.
- Notice of Privacy Practices.
- Access policies and procedures.

When reviewing their efforts to implement an effective access process consistent with the Privacy Rule standard, covered entities may want to consider the following questions.

Covered Entity Access Policy and Procedures – Key Considerations[6]
Does your process and access request form (if you have one) make clear that the Privacy Rule generally requires the entity to provide individuals, upon request, with access to their medical and billing records that are maintained by the covered entity?
Does your process or form provide the individual a clear method or options for describing the PHI that is the subject of the request?
Does your process or form provide the individual with a choice of form and format for receiving the PHI, including the ability to request records in a particular electronic format?[7]
Does it provide the individual with the option to direct the entity to transmit an electronic copy of PHI in an electronic health record to a third party, and your duty to implement that request?[8]
Does it explain the required (30 day, with one 30 day extension when justified) timeline for response?[9]
Are your fees for providing access reasonable and cost-based, including only labor for copying, supplies for creating the copy, and postage? Does the fee structure address providing access in different forms and formats?[10]
Does your process or form explain the reasons you may deny an individual's request, and the steps involved in doing so?[11]

[6] For extensive guidance, *see* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
[7] § 164.524(c)(2).
[8] § 164.524(c)(3)(ii). *See* footnote 6.
[9] § 164.524(b)(2).
[10] § 164.524((c)(4).
[11] *See* § 164.524(a)(2) *Unreviewable grounds for denial*, (a)(3) *Reviewable ground for denial*.

Does it explain the appeals process the individual can use if their request is denied?[12]

FIGURE 11 COVERED ENTITY ACCESS POLICY AND PROCEDURES--KEY CONSIDERATIONS

AUDIT RESULTS:

Summary of P65 Analysis

Almost all covered entities audited (89%) failed to show they were correctly implementing the individual right of access. Certain themes recurred in their documentation.

- Inadequate documentation of access requests. Many covered entities stated that they had never received an access request. This suggests a possible misunderstanding of the standard, as it is common for a patient to request a copy of lab results, immunization records, or a copy of a bill. Some covered entities did not maintain adequate records of how and when it responded to a request. For example, one entity recorded no dates for the request or response. In another example, the entity responded more than 30 days after receipt of the request without following the written extension requirements.
- Insufficient evidence of policies for individuals to request and obtain access to PHI. For example, one entity provided a form used by patients to name an authorized representative as its access policy.
- Inadequate or incorrect policies and procedures for providing access.
    - Procedures that required individuals to submit signed authorization forms – which exceed what is required for a right of access request. Further, because an entity is not required by the Privacy Rule to disclose records pursuant to an authorization, requiring authorization forms for right of access requests implies that the entity can ignore a request for access without following the required procedures for a written denial, such as providing the individual with written notice and informing the individual of the right to request a review of the denial decision.
    - Policies that incorrectly state that the entity could deny access to PHI in a designated record set, such as lab test results,[13] or prescription medication history.
    - Lack of policies for honoring requests for information to be provided to a designated third party.[14]
    - No provision to enable an individual to state her desired form and format for receiving the PHI, such as a particular electronic form. For example, a request form that limited the choices to fax, mail, or in office pick up.
    - Policy that did not address situations where a patient requests access to records not maintained by the entity.

[12] § 164.524(a)(3) *Reviewable ground for denial*, and (a)(4) *Review of a denial of access*; also § 164.524(d) *Implementation specifications: Denial of access.*

[13] As of October 6, 2014, individuals have the right to access test reports directly from clinical laboratories subject to HIPAA and, as of January 23, 2020, when the covered entity uses or maintains an electronic health record, to direct that electronic copies of those test reports be transmitted to persons or entities designated by the individual. *See* https://www.hhs.gov/hipaa/for-professionals/special-topics/clia/index.html, and footnote 6.

[14] *See* footnote 6 regarding *Ciox Health, LLC v. Azar, et al.*, which held that the individual's right to direct PHI to a third party is limited to *an electronic copy of PHI in an electronic health record.* The court also held that the reasonable, cost-based fee limitation does not apply when directing PHI to a third party.

- Lack of a clear reasonable cost-based fee policy or application of blanket fees in violation of the standard.
- Failure to maintain policies and procedures requiring a timely written denial and the basis for denying an access request.
- NPP did not correctly describe individual rights.
- NPP did not identify or incorrectly identified the patient's right to timely access (*i.e.*, within 30 days of request unless an extension is provided). Many covered entities stated incorrectly that the entity had 60 days, instead of 30 days, to respond to requests.

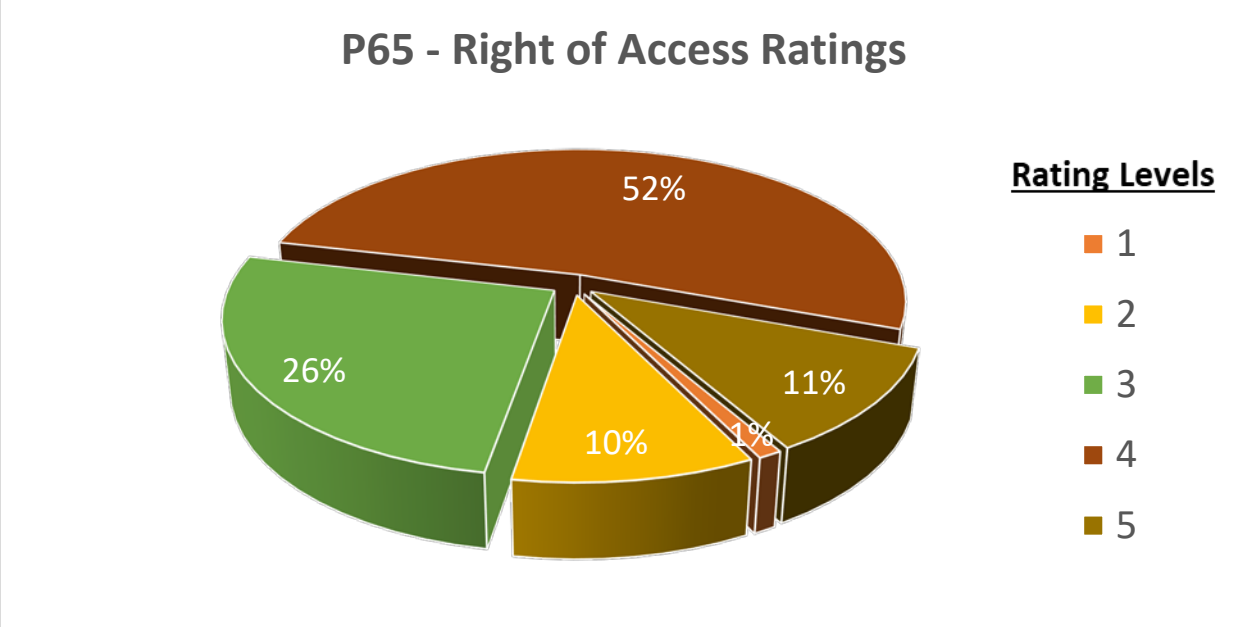

FIGURE 12 RIGHT OF ACCESS

Only one audited entity received a 1 rating for its access implementation. The table below includes OCR's description of submitted documentation that indicated implementation of an appropriate individual access process. Covered entities may consider whether their own processes for enabling the right of access could be documented at this level.

Example Documentation of an Individual Access Process
❖ *Adequate Evidence of Access Requests* -- The evidence of fulfilled access requests included a summary list of five requests from 2015 and the five request forms and related screenshots. The entity fulfilled each request within 30 days, most were filled within one day of receipt. The entity submitted documentation of the access requests, which showed how many pages of records were sent and how the individual obtained the records.
❖ *Notice of Privacy Practices* – The NPP addressed the patient's rights to obtain access to their health records, and stated the timeframe in which the entity must provide a response to an access request.

- *Authorization for Release template* was designed in part for individuals to request access to their own records. It also gave individuals an opportunity to specify the form or format of the records they request.
- *Authorization to Disclose Patients' PHI Policy* – The policy identified the individual's right to access their own health records. It further addressed timeframes in which the entity must respond to requests (including extensions); the process to honor an individual's request to access medical records in a specific form or format; the procedure for addressing requests for records that the entity no longer possesses; how and when fees will be charged for fulfilling a request; and the procedure taken to process request denials.

FIGURE 13 EXAMPLE DOCUMENTATION OF AN INDIVIDUAL ACCESS PROCESS

ENTITY RESPONSE: Seventy-four covered entities audited on this element responded to the draft report; 64 agreed or adopted the recommendations; one stated it had misinterpreted the law when conducting their compliance activities or the request for documentation, and either provided insufficient or no documents for review.

POSITIVE OUTCOMES: As evidenced by the number of covered entities that agreed with or adopted the findings, covered entities were receptive to the audit, welcomed the findings, and expressed the desire to comply with the law.

OPPORTUNITIES FOR IMPROVEMENT: OCR and the Office of the National Coordinator for Health Information Technology (ONC) have developed many aids for covered entities seeking to improve their patient records request process. One is ONC's Improving the Health Records Request Process for Patients (pictured below). Another is the audit protocol itself, which provides detailed audit inquiry language that sets forth OCR's expectations of entity performance in complying with the standard. More links to helpful tools are available in the appendix. Covered entities can review their policies and procedures against the list of questions provided in the table above and revise as necessary. OCR's access guidance is also a good source for answers to particular questions covered entities might have about necessary policies. Improvement to documentation of access provision is critical. Staff involvement in development of the procedures and consistent training may be helpful to improve fulfillment of individual access rights.

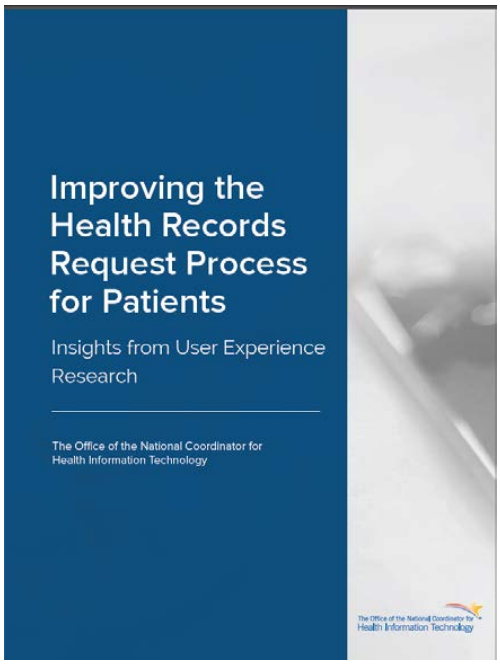

FIGURE 14 IMPROVING THE HEALTH RECORDS REQUEST PROCESS FOR PATIENTS

ELEMENT – TIMELINESS OF NOTICE OF BREACH NOTIFICATION (BNR12)

AUDIT REQUIREMENTS:

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400 to 164.414, requires HIPAA covered entities and business associates to provide notification following a breach of unsecured PHI. A *breach* is the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI.[15] Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Under the timeliness of individual notification requirement at 45 CFR § 164.404(b), generally a covered entity shall provide the notification to an individual without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.[16] See 45 CFR § 164.404(b).

DOCUMENTS REQUESTED:

- Individual notice and other documentation for five breach incidents affecting fewer than 500 individuals.

AUDIT RESULTS:

OCR reviewed documentation of breach incidents affecting fewer than 500 individuals. Documentation reviews included the date the breach occurred, the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification. The majority (71%) of audited covered entities issued notices to individuals within the regulatory timeframe.

[15] *See* definition of Breach in § 164.402.
[16] Except as provided in § 164.412.

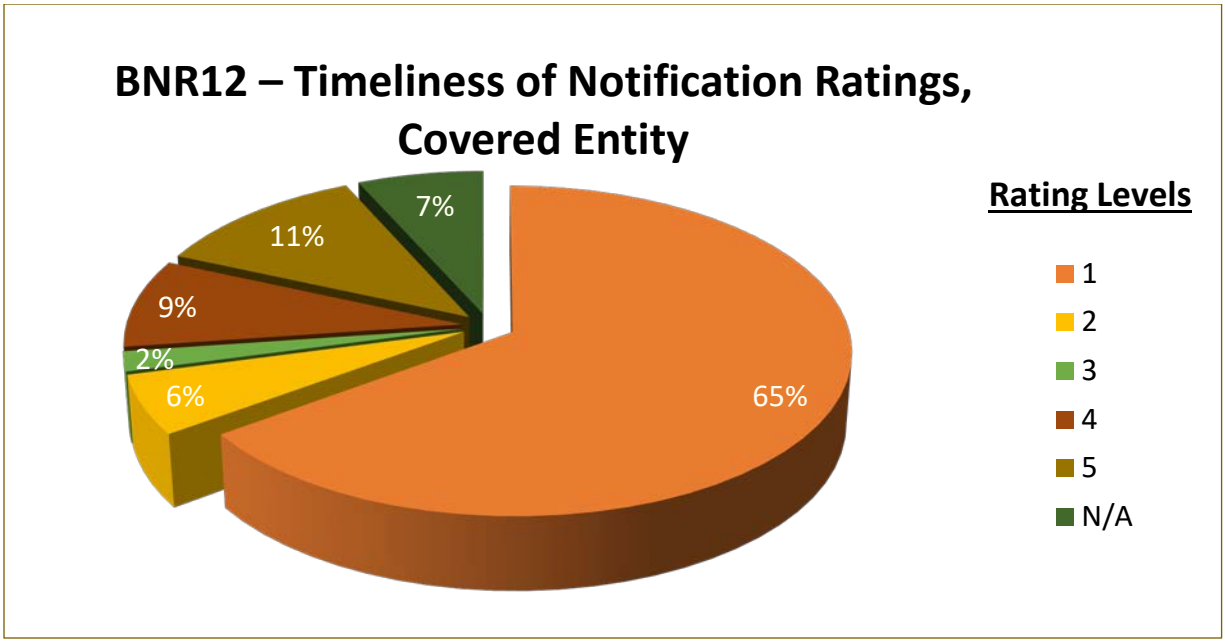

FIGURE 15 TIMELINESS OF NOTIFICATION RATINGS, COVERED ENTITY

ENTITY RESPONSE: Twenty-eight covered entities audited on this element responded to the draft report; 20 agreed or adopted the recommendations; four stated they had misinterpreted the law when conducting their compliance activities or the request for documentation, and either provided insufficient documents or did not provide any document for review.

POSITIVE OUTCOMES: The OCR breach guidance web page and the Audit Protocol proved to be useful resources for covered entities seeking further clarity on documentation.

OPPORTUNITIES FOR IMPROVEMENT: Since some covered entities did not meet the timeliness requirement, they should ensure that procedures are in place to identify and respond to breaches within the required time frame.

ELEMENT – CONTENT OF BREACH NOTIFICATION (BNR13)

AUDIT REQUIREMENTS:

To assess compliance with 45 CFR § 164.404(c)(1), the Content of Breach Notification element, OCR inquired whether the covered entity used a standard template or form letter for notification to individuals for breaches or for specific types of breaches. If the covered entity used such a form or template, OCR evaluated whether they included the required content. OCR further requested and examined a list of breaches, if any, which occurred in the previous calendar year. OCR obtained and reviewed a copy of a single written notice sent to affected individuals for each breach incident in the previous calendar year. For the first five breach incidents that occurred in the previous calendar year, OCR obtained and evaluated documentation related to the required content in the written notices sent to affected individuals. See 45 CFR § 164.404(c)(1).

Breach Notification to Individuals Must be Written in Plain Language & Include:
• A brief description of the breach, including dates of breach and breach discovery, if known
• A description of the types of information that were involved in the breach
• The steps affected individuals should take to protect themselves from potential harm
• A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches
• Contact information for the covered entity (or business associate, as applicable) such as a toll-free telephone number, an email address, website, or postal address

FIGURE 16 REQUIRED BREACH NOTIFICATION CONTENT 45 CFR § 164.404(c)

DOCUMENTS REQUESTED:

- Documentation of five breach incidents affecting 500 or more individuals.
- Breach templates and/or forms.
- Copy of a single written notice for each breach incident.

AUDIT RESULTS:

Summary of BNR13 Analysis:

Most covered entities (67%) submitted notification letters to individuals that were missing one or more pieces of required content. The more frequently omitted content requirements included:

- A description of the types of unsecured PHI that were involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved.
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- An explanation of the entity's investigation and mitigation activities. The standard requires more detail than the frequently stated, "we investigated and took appropriate action."
- Several covered entities could not document compliance because they did not provide dates on the letters and documentation.
- Inadequate contact information. For example, several notification letters omitted contact procedures for individuals to ask questions or learn additional information, such as a toll-

free telephone number, an email address, website, or postal address. Some entities provided only a telephone number as contact information, which was not a toll-free number as required.

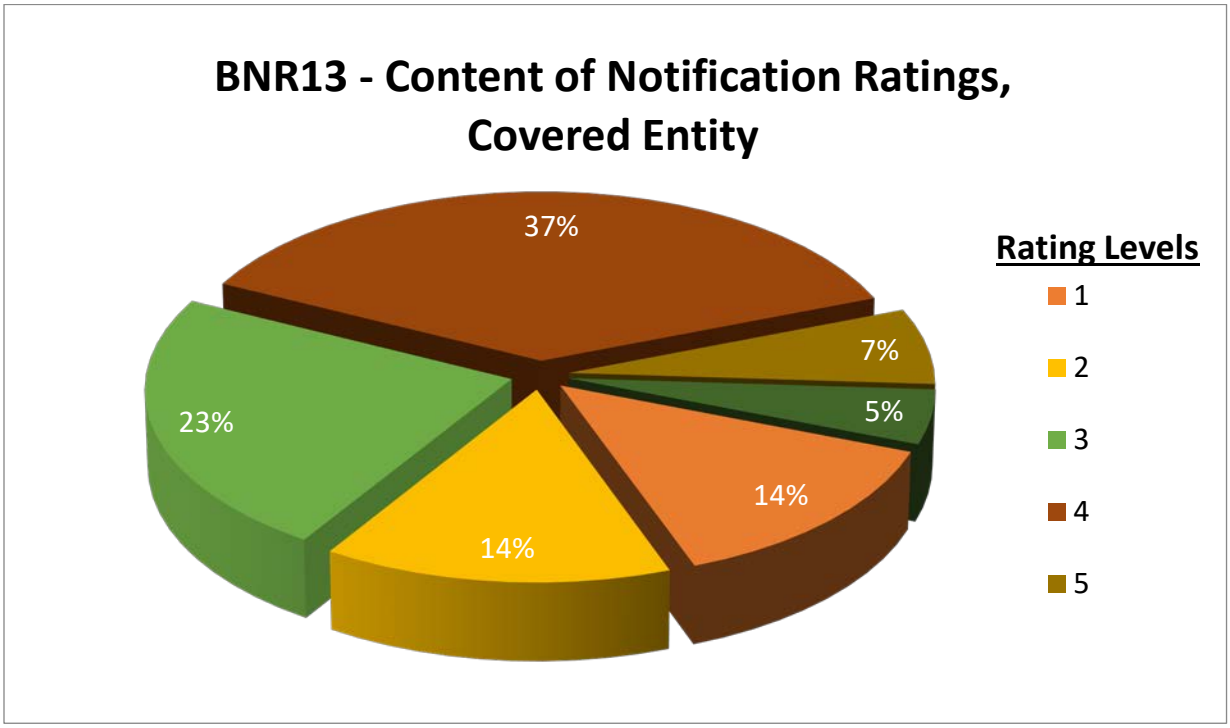

FIGURE 17 CONTENT OF NOTIFICATION RATINGS, COVERED ENTITY

ENTITY RESPONSE: Five entities reported that they had not experienced a breach and are listed on the chart as N/A. Forty-two covered entities audited on this element responded to the draft report by agreeing to or adopting the recommendations; 15 stated they had misinterpreted the law when conducting their compliance activities or the request for documentation, and either provided insufficient documents or did not provide any document for review.

POSITIVE OUTCOMES: Several covered entities, upon review of the audit draft report, adopted the recommendations and immediately incorporated these changes into their organization.

OPPORTUNITIES FOR IMPROVEMENT: Covered entities must ensure that all staff are properly trained on requirements, notification letters contain all the provisions outlined in the regulation and that they establish procedures to properly document and keep affected individuals informed.

ELEMENT –BREACH NOTIFICATION BY A BUSINESS ASSOCIATE TO A COVERED ENTITY (BNR17)

AUDIT REQUIREMENTS:

The Breach Notification Rule provides the standard for a business associate to follow when reporting a breach to a covered entity. See 45 CFR § 164.410.

Breach Notification Requirements for Business Associates
• Business associate must notify the covered entity following discovery of a breach
• Business associate must provide notice to the covered entity without unreasonable delay and no later than 60 calendar days from the discovery
• Covered entity & business associate may negotiate stricter timeframes for the business associate to report
• To extent possible, business associate must identify each individual affected and include any other available information required for notification to individuals
• While a covered entity ultimately maintains the obligation to notify, where a breach occurs at or by its business associate, a covered entity may delegate the responsibility of providing the required notifications to that business associate or another business associate
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

FIGURE 18 BREACH NOTIFICATION REQUIREMENTS FOR BUSINESS ASSOCIATES

DOCUMENTS REQUESTED:

- Notifications of breaches sent by the business associate to the covered entity.

AUDIT RESULTS:

Of the forty-one (41) business associates audited, 32 (78%) stated that they had never experienced a breach of PHI.

Of the nine that reported potential breaches of PHI, most had provided the majority of the required information about the incidents to the covered entities within the 60-day deadline.

Required information that was frequently omitted was content to enable the covered entity to meet their breach notification obligations to affected individuals. The information most often

missing were the identities of the individuals whose information was involved in the breach and information about any steps they should take to protect themselves from potential harm. Failure to include required content in the breach notification could adversely impact the rights of the individuals who are affected by the breach, and could adversely impact their ability to protect themselves from harm. In a few cases, the business associates did not keep records sufficient to show that they made the notifications within the 60-day timeframe.

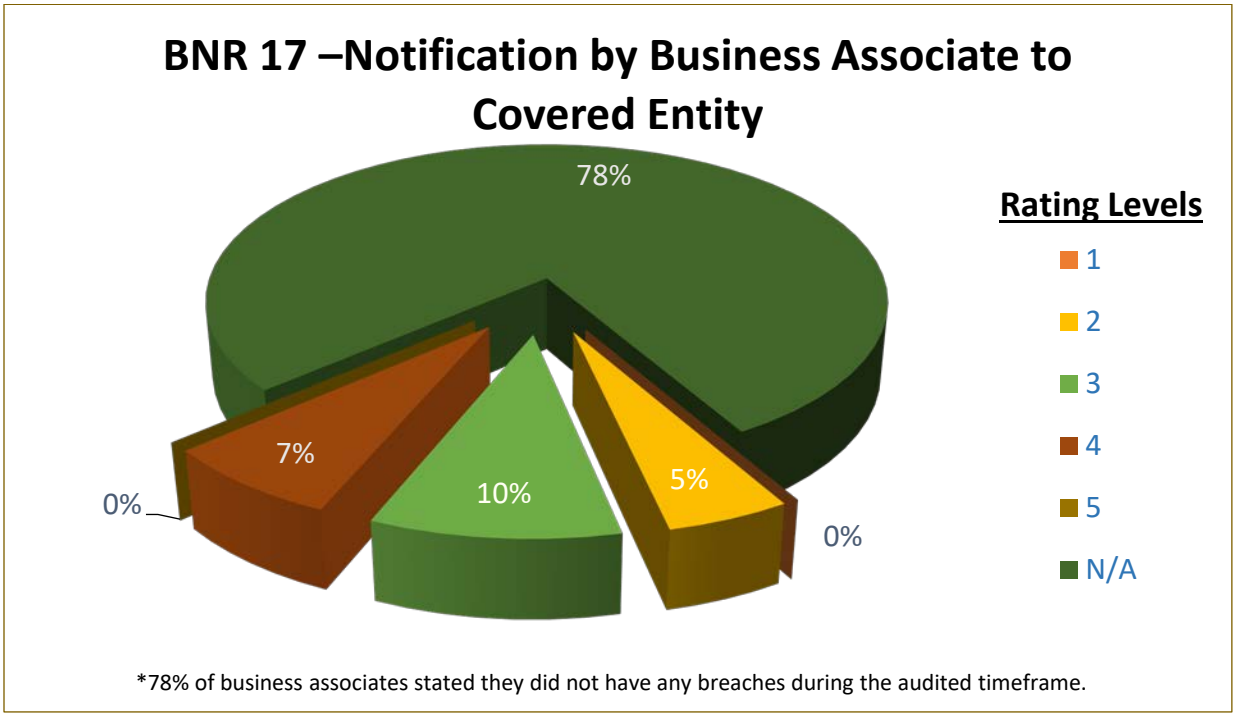

FIGURE 19 NOTIFICATION BY BUSINESS ASSOCIATE TO COVERED ENTITY

ENTITY RESPONSE: Four business associates audited on this element responded to the draft report; two agreed or adopted the recommendations; one stated it had misinterpreted the law when conducting their compliance activities or the request for documentation, and either provided insufficient documents or did not provide any document for review.

POSITIVE OUTCOMES: Upon review of the audit draft report, two business associates adopted the recommendations and immediately incorporated these changes into their operations. Those that reported breaches generally provided documentation of the information required for notification, such as the date the business associate discovered the breach, steps the business associate took to communicate about and investigate the breach, root cause analysis, the kind of PHI that was disclosed, remedial actions in response to the breach, and what happened to the PHI that was accessed.

OPPORTUNITIES FOR IMPROVEMENT: Many organizations that met the definition of a business associate communicated to OCR that they did not understand that they had breach notification responsibilities under the HIPAA Rules. See OCR guidance on business associates, and OCR's

Direct Liability of Business Associates. Many may also want to concentrate their efforts on recognizing security incidents that are breaches of PHI.

ELEMENT – SECURITY RISK ANALYSIS (S2)

AUDIT REQUIREMENTS:

A covered entity or business associate must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity. As a foundation for this risk analysis, the entity must identify all of the ePHI created, maintained, received or transmitted by the organization. Entities were asked to provide evidence that they had conducted a risk analysis and provide their policies and procedures for conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains or transmits. See 45 CFR § 164.308(a)(1)(ii)(A).

DOCUMENTS REQUESTED:

- Current and prior risk analyses and results.
- Policy and procedures of the risk analysis process.
- Policies and procedures related to the implementation of risk analysis.
- Documentation demonstrating implementation of risk analysis process, how it is available to persons responsible for the process, and evidence the documentation is periodically reviewed and updated, as needed.

AUDIT RESULTS:

Consistent with the findings of OCR's compliance reviews and complaint investigations, these audits confirmed that small percentages of covered entities (14%) and business associates (17%) (Categories 1 and 2, respectively) are substantially fulfilling their regulatory responsibilities to safeguard ePHI they hold through risk analysis activities. Entities generally failed to:

- Identify and assess the risks to all of the ePHI in their possession.
- Develop and implement policies and procedures for conducting a risk analysis.
- Identify threats and vulnerabilities, to consider their potential likelihoods and impacts, and to rate the risk to ePHI.
- Review and periodically update a risk analysis in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.
- Conduct risk analyses consistent with policies and procedures.

Failing to document any efforts to develop, maintain and update policies and procedures, and to use them to conduct risk analyses, was common.

- Some entities provided irrelevant documentation, such as a document that describes a patient's insurance prescription coverage and rights; a document that discusses pharmacy fraud, waste and abuse; and a conflict of interest and code of conduct employee sign-off page.

- Providers commonly submitted documentation of some security activities of a third party security vendor, but no documentation of any risk analysis that served as the basis of the activities.
- Entities offered third party template policy manuals that contain no evidence of entity-specific review or revision and no evidence of implementation.

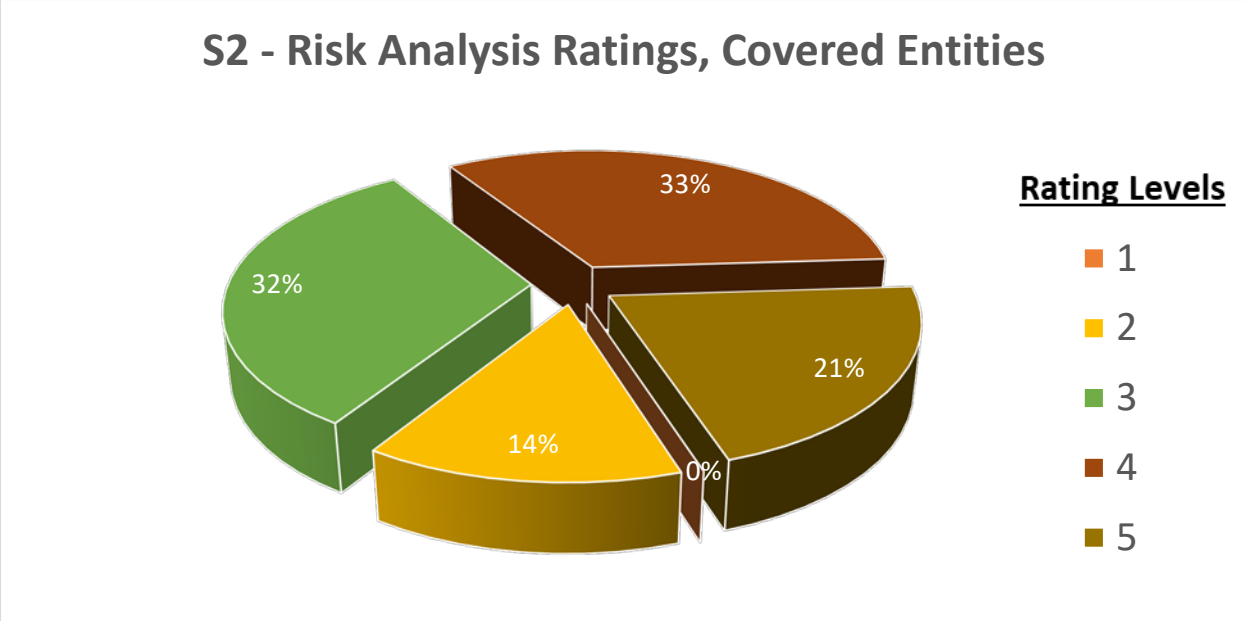

FIGURE 20 RISK ANALYSIS RATINGS, COVERED ENTITY

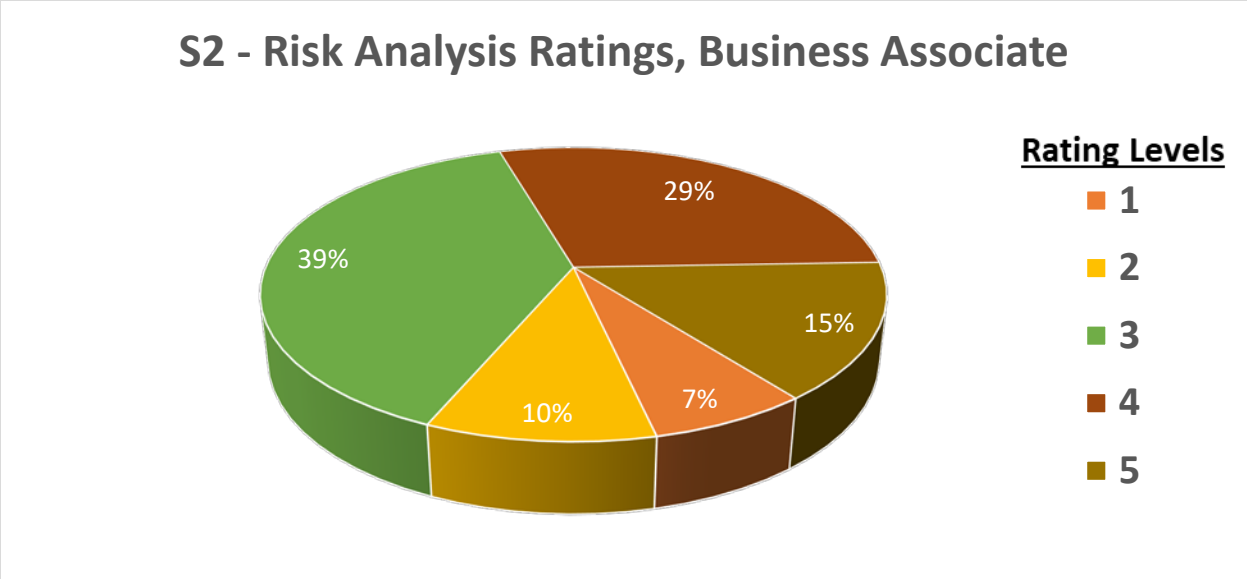

FIGURE 21 RISK ANALYSIS RATINGS, BUSINESS ASSOCIATE

ENTITY RESPONSE: Fifty-six entities audited on this element responded to the draft reports; 28 agreed or adopted the recommendations; 20 stated they had misinterpreted the law when conducting their compliance activities or the request for documentation, and either provided insufficient documents or did not provide any document for review.

POSITIVE OUTCOMES: Many entities made attempts to establish a risk analysis program. OCR requested information from various points in time to determine whether entities were meeting the requirements for regular updating and implementation. Some entities made significant improvements in their safeguards over the years. For example, one small provider submitted evidence of an inadequate risk analysis for 2010, a much improved version in 2013, and a comprehensive and detailed analysis in 2015. In response to the draft findings OCR shared with the entities, many submitted detailed plans for improvements.

OPPORTUNITIES FOR IMPROVEMENT: Many entities utilize and rely on outside agencies to manage or perform risk analyses for their organizations; however, these companies frequently failed to meet the requirements. Entities incorrectly assumed that a purchased security product satisfied all Security Rule requirements. The responsibility to maintain an appropriate risk analysis rests with the entity. It is essential that entities understand and comply with risk analysis requirements in order to appropriately safeguard PHI.

Several sources of guidance are available for developing risk management programs that include risk analysis. OCR, ONC and the National Institute of Standards and Technology (NIST) offer technical assistance for covered entities and business associates.

ELEMENT – SECURITY RISK MANAGEMENT (S3)

AUDIT REQUIREMENTS:

The Risk Management Standard requires implementation of security measures *sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level*. OCR asked entities to provide evidence to demonstrate that they had policies and procedures in place for a sufficient risk management process. They were also asked to submit evidence to demonstrate that they had implemented sufficient security measures. See 45 CFR § 164.308(a)(1)(ii)(B).

DOCUMENTS REQUESTED:

- Documentation demonstrating the efforts used to manage risks.
- Policies and procedures of the risk management process.
- Policies and procedures related to the implementation of risk management.
- Documentation demonstrating that current and ongoing risks are reviewed and updated.
- Documentation demonstrating implementation of the risk management process, how it is available to persons responsible for the process, and evidence the documentation is periodically reviewed and updated, as needed.

AUDIT RESULTS:

In these audits, OCR found the same failures to manage identified risk that are seen in OCR's compliance reviews and complaint investigations. Because audited entities largely failed to conduct appropriate risk analyses, they were then unable to link their security plans to management of identified risks. Conversely, some entities had identified risks but failed to respond and implement appropriate security measures. Ninety-four percent of covered entities and 88% of business associates failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level (Categories 3-5).

- Entities lacked the necessary focus on technical safeguards (access controls, audit controls, etc.) needed to properly protect the confidentiality, integrity, and availability of ePHI.
- The policies and procedures provided in support of the risk analysis and risk management requirements indicate entity misunderstanding of the importance of determining acceptable levels of risk, what specific vulnerabilities were applicable to their environment, or how to mitigate the risks or vulnerabilities to ePHI throughout their organization.
- Entities that demonstrated some—although incomplete—evidence of risk management commonly submitted documentation they maintained to satisfy the security risk analysis measure of the Promoting Interoperability Program (formerly known as the Medicare and Medicaid EHR Incentive Programs) for eligible hospitals and critical access hospitals (CAHs) as well as the security risk analysis measure of the Merit-based Incentive Payment System (MIPS) Promoting Interoperability performance category (formerly

known as the Advancing Care Information performance category). Such documentation is incomplete because the scope of the security risk analysis measure for the Promoting Interoperability Program relates only to ePHI created or maintained using certified electronic health record technology (CEHRT), and does not assess the potential risks and vulnerabilities to other ePHI created, received, maintained, or transmitted by the covered entity.[17]

- In some instances, encryption was included as part of a remediation plan, but was not carried out or was not implemented within a reasonable timeframe.
- One entity had implemented an appropriate risk management plan in 2013, but failed to conduct any updates since that time.

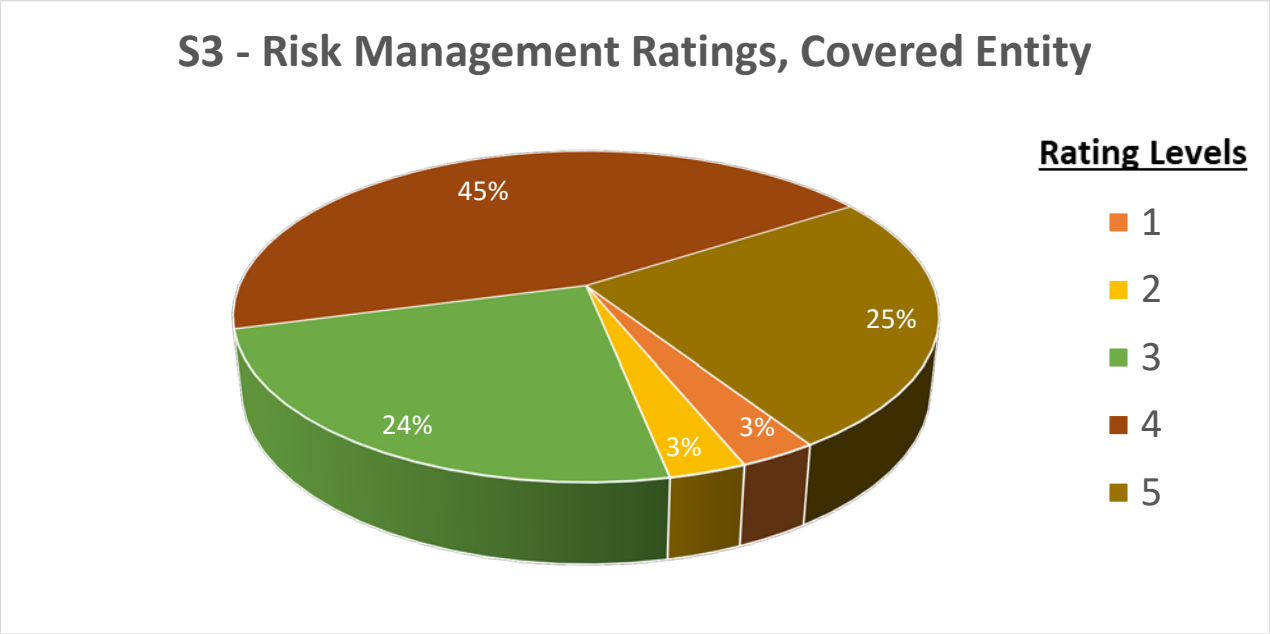

FIGURE 22 SECURITY RISK MANAGEMENT RATINGS, COVERED ENTITY

[17] The Promoting Interoperability Programs encourage eligible professionals (EPs) and eligible hospitals and CAHs to adopt, implement, upgrade, and demonstrate meaningful use of CEHRT. In prior rulemaking, CMS noted that, consistent with HIPAA and its implementing regulations, protecting ePHI remains essential to all aspects of meaningful use under the Promoting Interoperability Programs (80 FR 62826). Therefore, CMS created a meaningful use core objective aimed at protecting patients' health care information. The "Protect Patient health information" objective is to protect electronic protected health information (ePHI) created or maintained by the CEHRT through the implementation of appropriate technical, administrative, and physical safeguards (42 CFR 495.24). Its associated measure, the security risk analysis measure, requires providers to conduct or review a security risk analysis in accordance with the requirements under the HIPAA Security Rule. For more information about CMS's Promoting Interoperability Program and Quality Payment Program, as well as the Security Risk Analysis measure, *see* https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html and https://www.govinfo.gov/content/pkg/FR-2018-11-23/pdf/2018-24170.pdf.

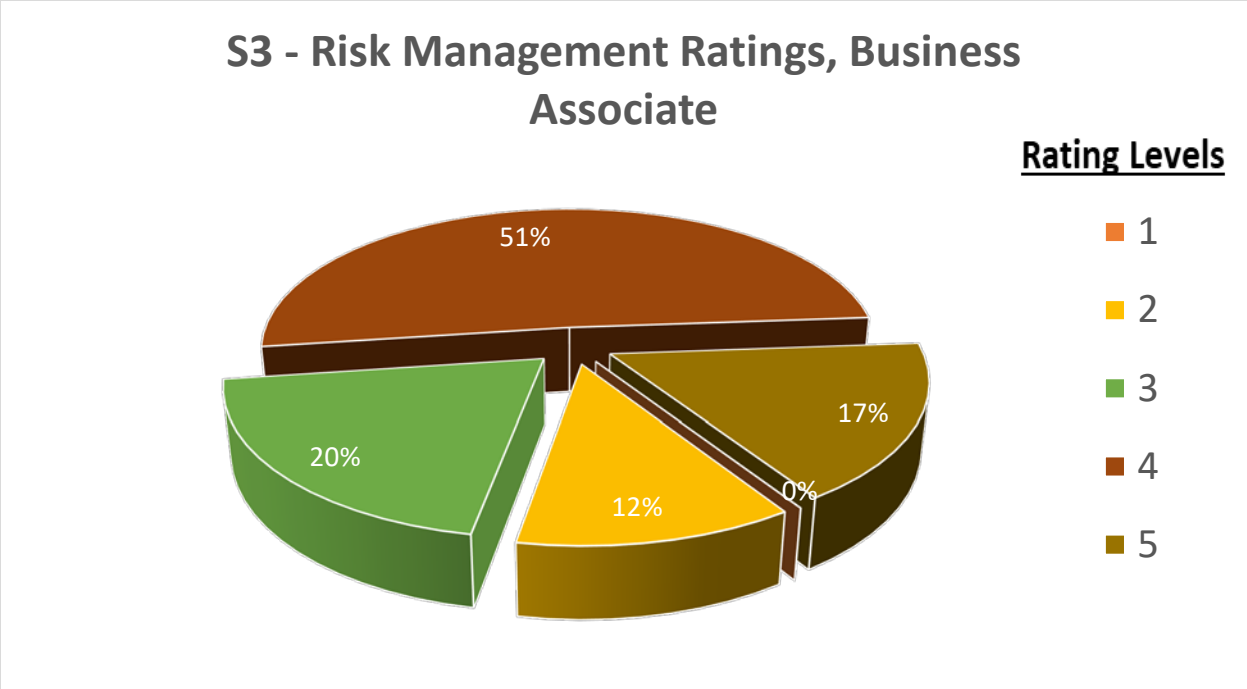

FIGURE 23 SECURITY RISK MANAGEMENT RATINGS, BUSINESS ASSOCIATE

COMPARISON OF RESULTS BETWEEN TYPES OF ENTITIES

Both covered entities and business associates must implement the risk analysis and risk management provisions of the Security Rule. As noted in the figures below, business associates were slightly more likely to have submitted documentation that indicated compliance with the risk analysis implementation specification (*i.e.*, a rating of one or two) than were covered entities (17% versus 14%). Likewise in risk management, 12% of business associates were rated 1 or 2, versus 6% of covered entities.

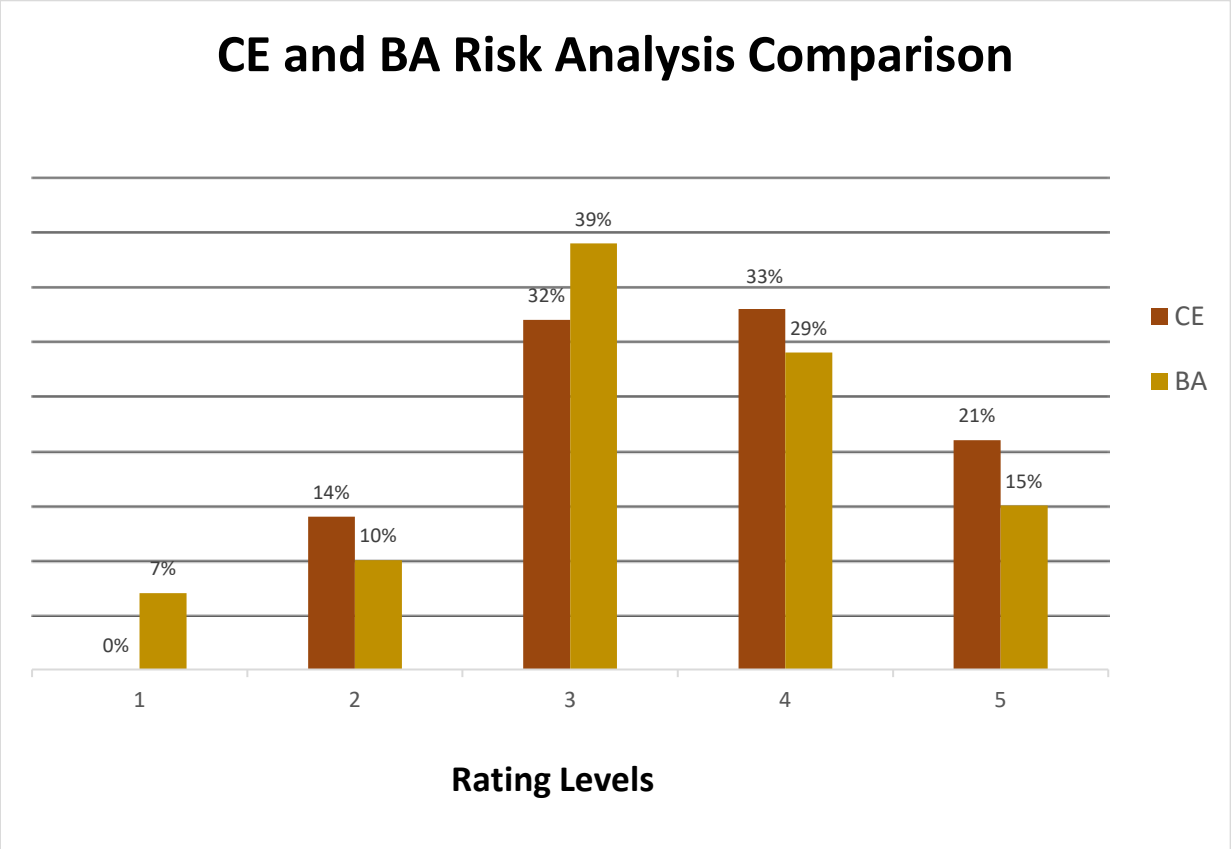

FIGURE 24 RISK ANALYSIS RATINGS COMPARISON, COVERED ENTITY (CE) AND BUSINESS ASSOCIATE (BA)

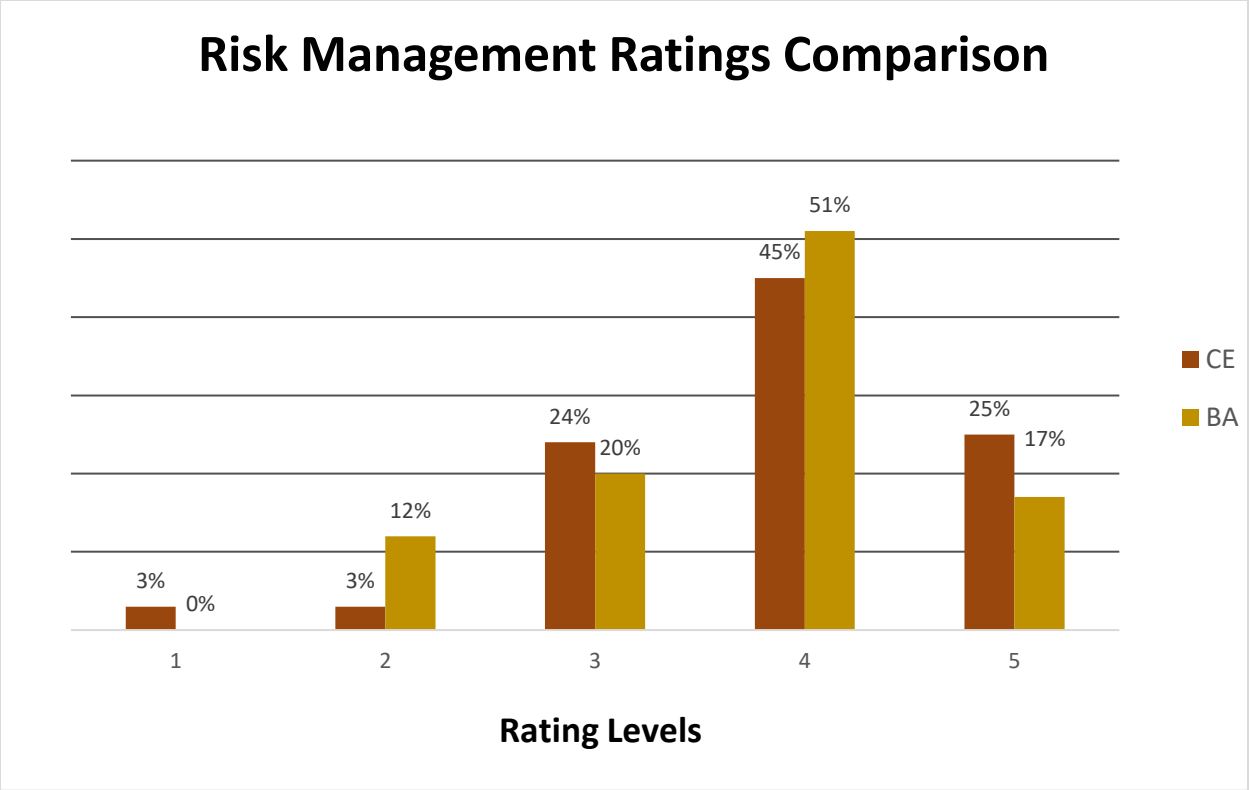

FIGURE 25 RISK MANAGEMENT RATINGS COMPARISON, COVERED ENTITY (CE) AND BUSINESS ASSOCIATE (BA)

ENTITY RESPONSE: Fifty-three entities audited on this element responded to the draft report; 21 agreed or adopted the recommendations; 20 stated they had misinterpreted the law when conducting their compliance activities or the request for documentation, and either provided insufficient documents or did not provide any document for review.

POSITIVE OUTCOMES: Entities reported making attempts to establish a risk management program.

OPPORTUNITIES FOR IMPROVEMENT: As noted in OCR's comments, most entities failed to produce policies and procedures, or implement security measures, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Reliance on contracted security firms does not relieve entities of their responsibility to establish a program that is compliant with the law. Entities can find resources for implementing appropriate risk management programs in the Appendix.

CONCLUSION

This report presents information about OCR's Phase 2 audits, the achievements and weaknesses identified, and methods audited entities may adopt, modify, and implement to strengthen compliance.

- Notices of Privacy Practices are often missing elements – using an HHS model notice to help them prepare a compliant NPP may assist covered entities to avoid that mistake.
- Most audited covered entities prominently post their Notices of Privacy Practices on their websites.
- Covered entities are not consistently providing individual access under the Privacy Rule—they can improve by implementing better procedures and digital technology using HHS technical assistance.
- The majority of audited covered entities issued breach notifications to individuals within the regulatory deadline.
- Both covered entities and business associates failed to implement effective risk analysis and risk management activities to safeguard ePHI. Among other resources, smaller covered entities and business associates can use the updated Security Risk Assessment Tool released by HHS in 2018 to assist them with required risk management activities.

APPENDIX

ENABLING ACCESS – OCR & ONC RESOURCES

For Providers

- OCR HIPAA Audit Protocol
- HIPAA Access Right Guidance and FAQs[18]
- Guide to Privacy and Security
- Improving the Health Records Request Process for Patients
- Resources for Mobile Health Apps Developers
- OCR and ONC YouTube pages
- Patient Portals Guidance in the Patient Engagement Playbook
- Provider Playbook API Information & API education video
- Model Notice of Privacy Practices

For Individuals

- Your Rights Under HIPAA and HealthIT.gov/Access for Access videos & factsheets
- OCR and ONC YouTube pages
- Information is Powerful Medicine
- Trusted Exchange Highlights for Patients

RISK ANALYSIS– OCR & ONC RESOURCES

- OCR Security Risk Analysis Guidance
- NIST HIPAA Security Rule Tool Kit
- ONC/OCR Security Risk Assessment Tool
- NIST SP 800-30 (Guide for Conducting Risk Assessments)

[18] See footnote 6 regarding *Ciox Health, LLC v. Azar, et al.*, which held that the individual's right to direct PHI to a third party is limited to *an electronic copy of PHI in an electronic health record.* The court also held that the reasonable, cost-based fee limitation does not apply when directing PHI to a third party.