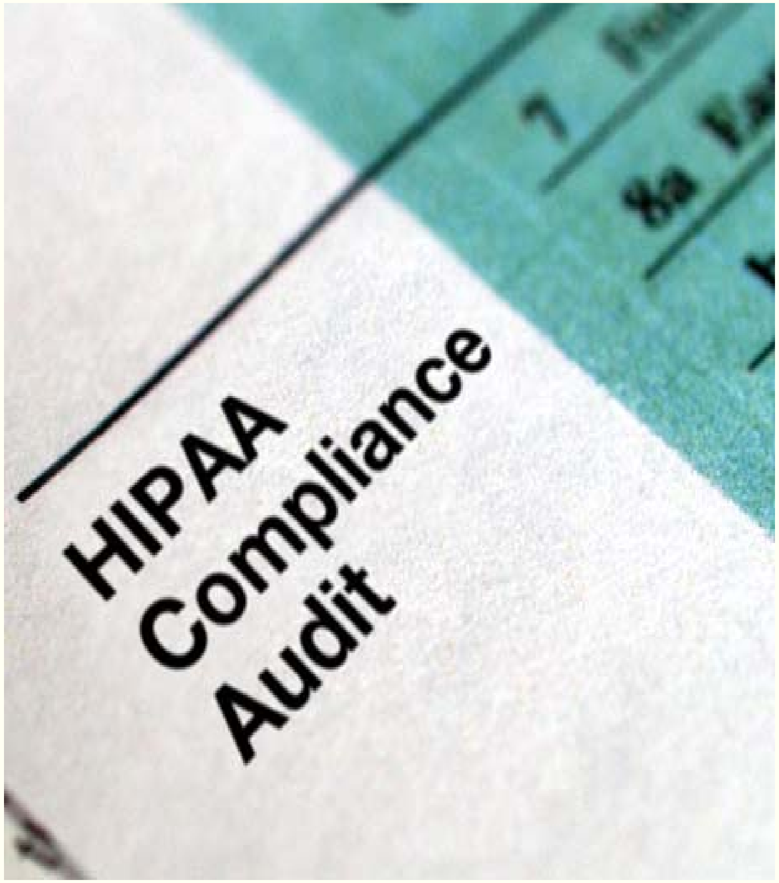
OCR HIPAA COMPLIANCE AUDIT PROGRAM:
THE RATINGS ARE IN



27th National HIPAA Summit

March 28, 2018

Zinethia L. Clemmons, MBA, MHA, RHIA, PMP
HIPAA Compliance Audit Program Director

Audit Program Purpose & Status

- Support Improved Compliance
- Identify best practices; uncover risks & vulnerabilities; detect areas for technical assistance; encourage consistent attention to compliance
    - Intended to be non-punitive, but OCR can open a compliance review
- Learn from this phase in structuring permanent audit program
- Develop tools and guidance for industry self-evaluation and breach prevention
- Desk audits of covered entities completed – Sept 2017
- Desk audits of business associates completed – Dec 2017

# of Audits by Type & Provision

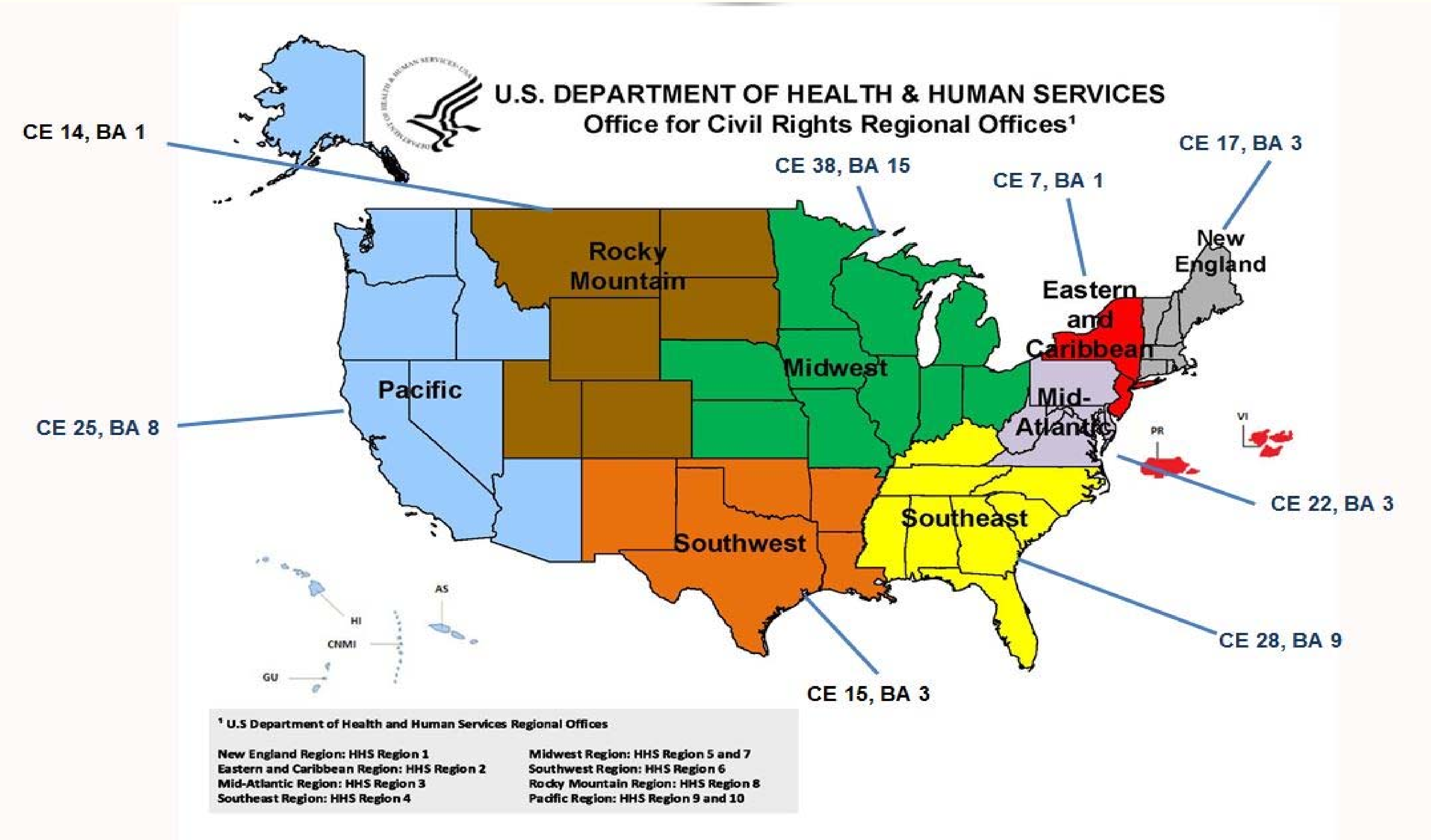
166 CE Audits

- Privacy and Breach (103)
- Security (63)

41 BA Audits

- Breach and Security (41)

# of Audits by Region



U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
Office for Civil Rights Regional Offices[1]

CE 14, BA 1

CE 38, BA 15

CE 7, BA 1

CE 17, BA 3

CE 25, BA 8

CE 22, BA 3

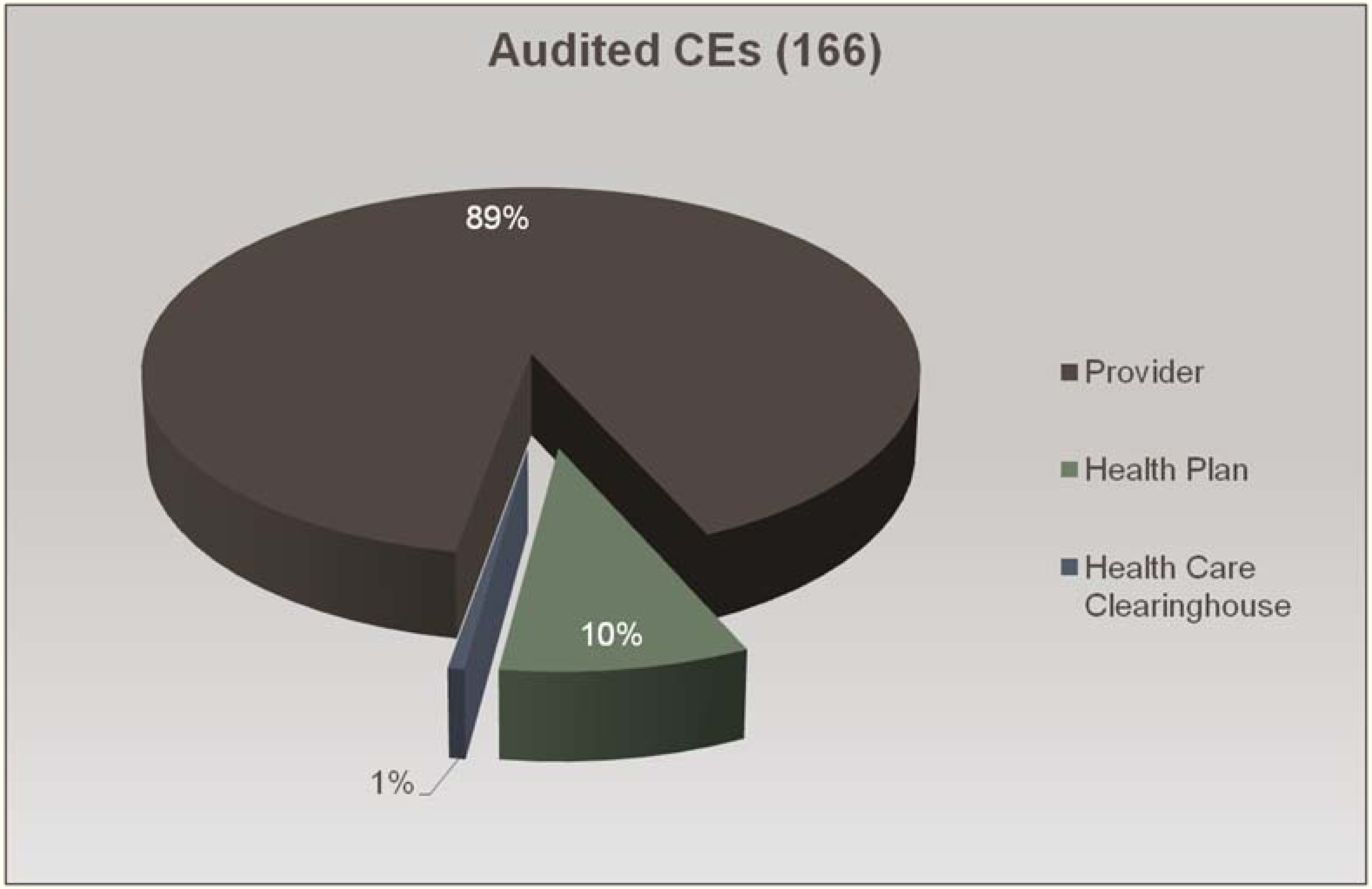
CE 28, BA 9

CE 15, BA 3

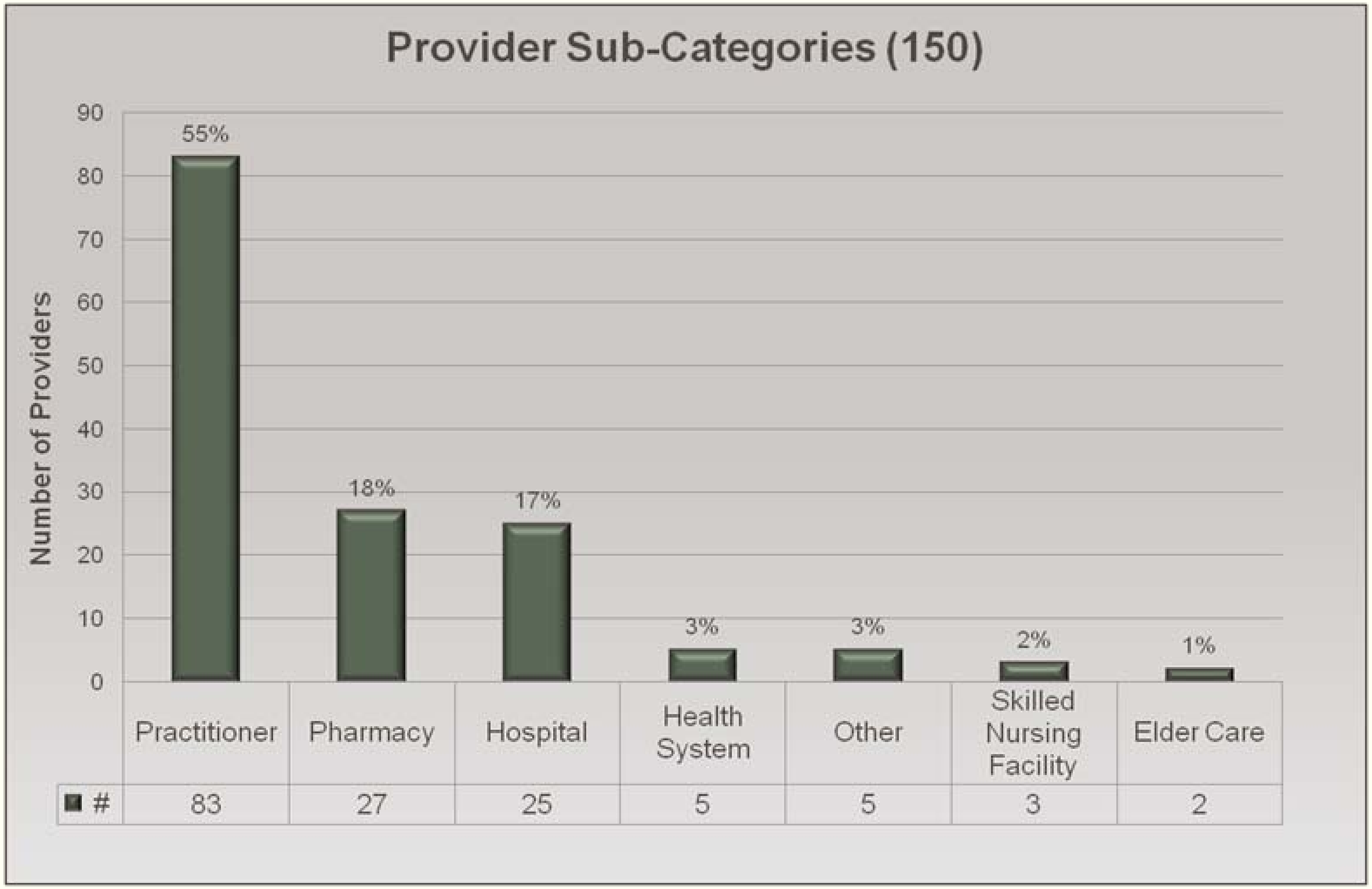
[1] U.S Department of Health and Human Services Regional Offices

New England Region: HHS Region 1
Eastern and Caribbean Region: HHS Region 2
Mid-Atlantic Region: HHS Region 3
Southeast Region: HHS Region 4
Midwest Region: HHS Region 5 and 7
Southwest Region: HHS Region 6
Rocky Mountain Region: HHS Region 8
Pacific Region: HHS Region 9 and 10

Audited Covered Entities



Audited Health Care Providers



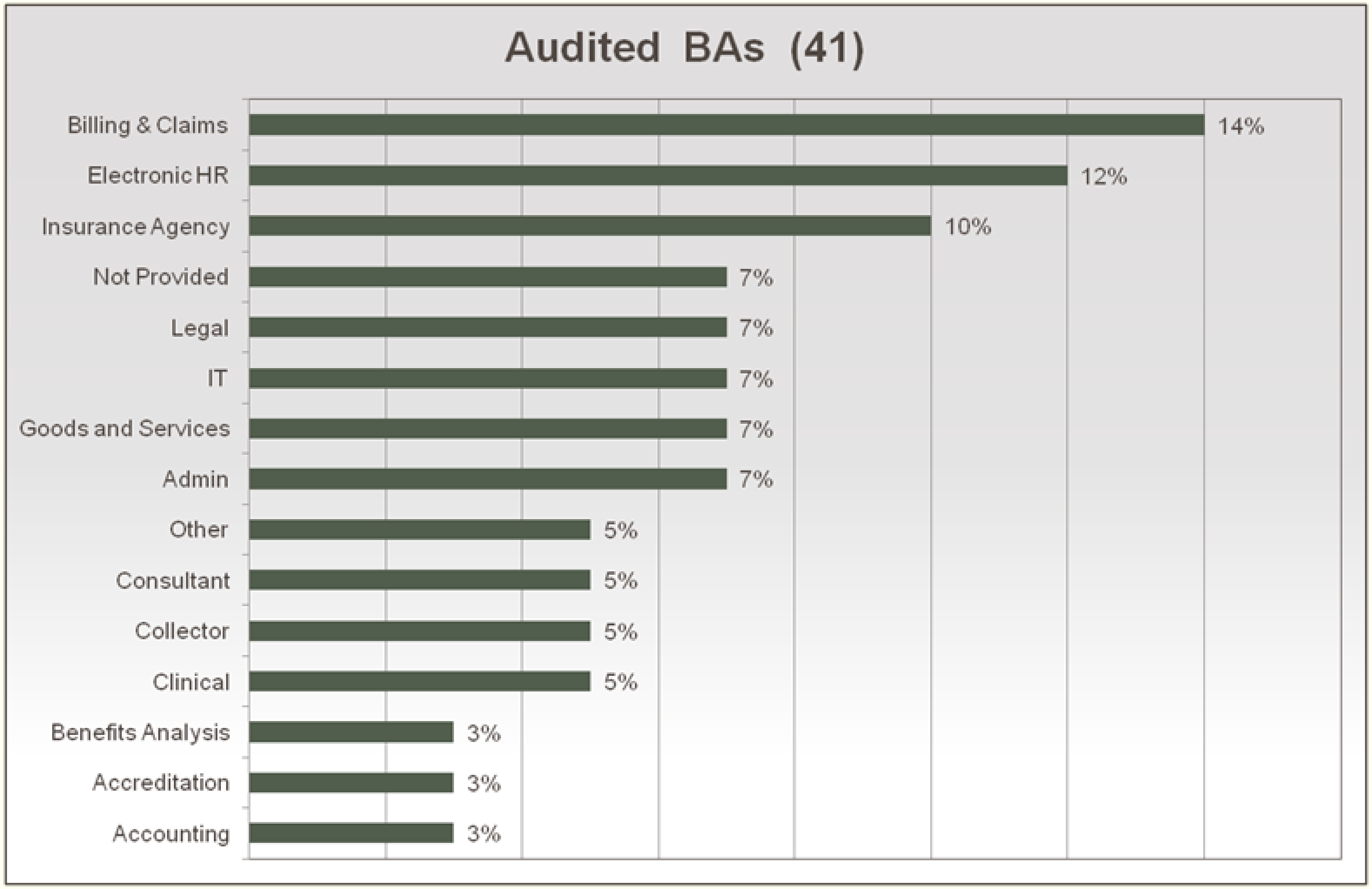
Provider Sub-Categories (150)

	Practitioner	Pharmacy	Hospital	Health System	Other	Skilled Nursing Facility	Elder Care
■ #	83	27	25	5	5	3	2

Covered Entity
Desk Audit Controls

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

Audited Business Associates



Business Associate
Desk Audit Controls

Breach Notification Rule Controls	Notification by a Business Associate [§164.410, with reference to Content of Notification §164.404(c)(1)]
Security Rule Controls	Security Management Process -- Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process -- Risk Management [§164.308(a)(1)(ii)(B)]

Document Requests:
Privacy & Breach

- Notice of Privacy Practices (NPP)
  - Copy of all notices including URL of notice posted on the entity web site, electronic notice policy and procedures
- Right to Access
  - Access requests, extensions to access requests, access requests templates/forms, NPP, access policies and procedures
- Timeliness of Notification
  - Five small and large breaches incidents
- Content of Notification
  - Five large breach incidents, breach template/form, copy of a single written notice

Document Requests: Security RA

- Risk Analysis
  - Current and prior risk analysis and results
  - Policies and procedures of the risk analysis process
  - Policies and procedures related to the implementation of risk analysis 6 years prior to the date of audit notification
  - Documentation from the previous year demonstrating implementation of risk management process, how it is available to persons responsible for the risk management process and evidence the documentation is periodically reviewed and updated, as needed

Document Requests: Security RM

- Risk Management
  - Documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment
  - Documentation demonstrating the efforts used to manage risks from the previous calendar year
  - Policies and procedures of the risk management process
  - Policies and procedures related to the implementation of risk management 6 years prior to the date of audit notification
  - Documentation demonstrating the current and ongoing risks reviewed and updated
  - Documentation from the previous year demonstrating implementation of the risk management process, how it is available to persons responsible for the risk management process and evidence the documentation is periodically reviewed and updated, as needed

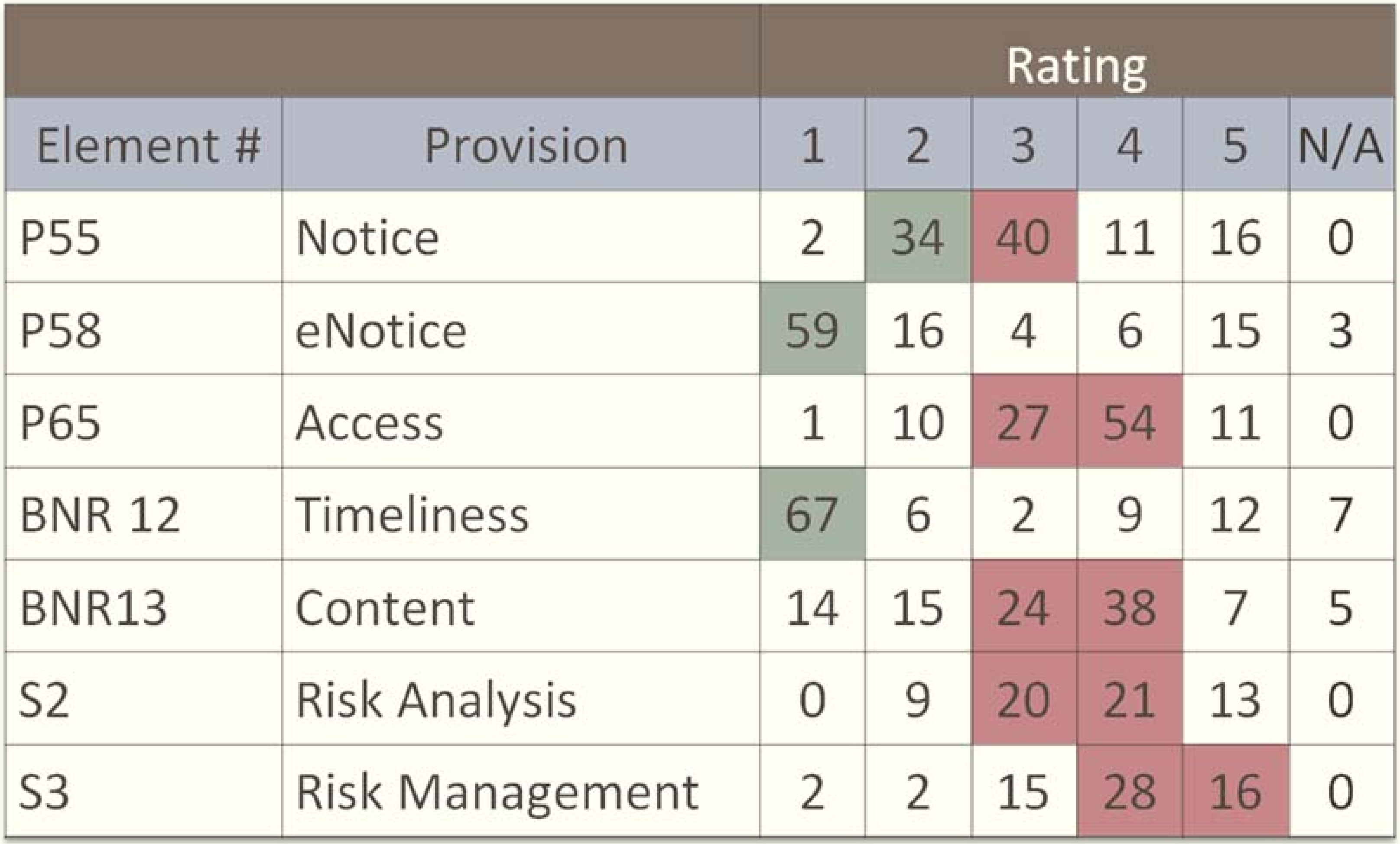
Ratings

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	Audit results indicate entity 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 serious attempt to comply with the Rules and enable individual rights with regard to PHI.

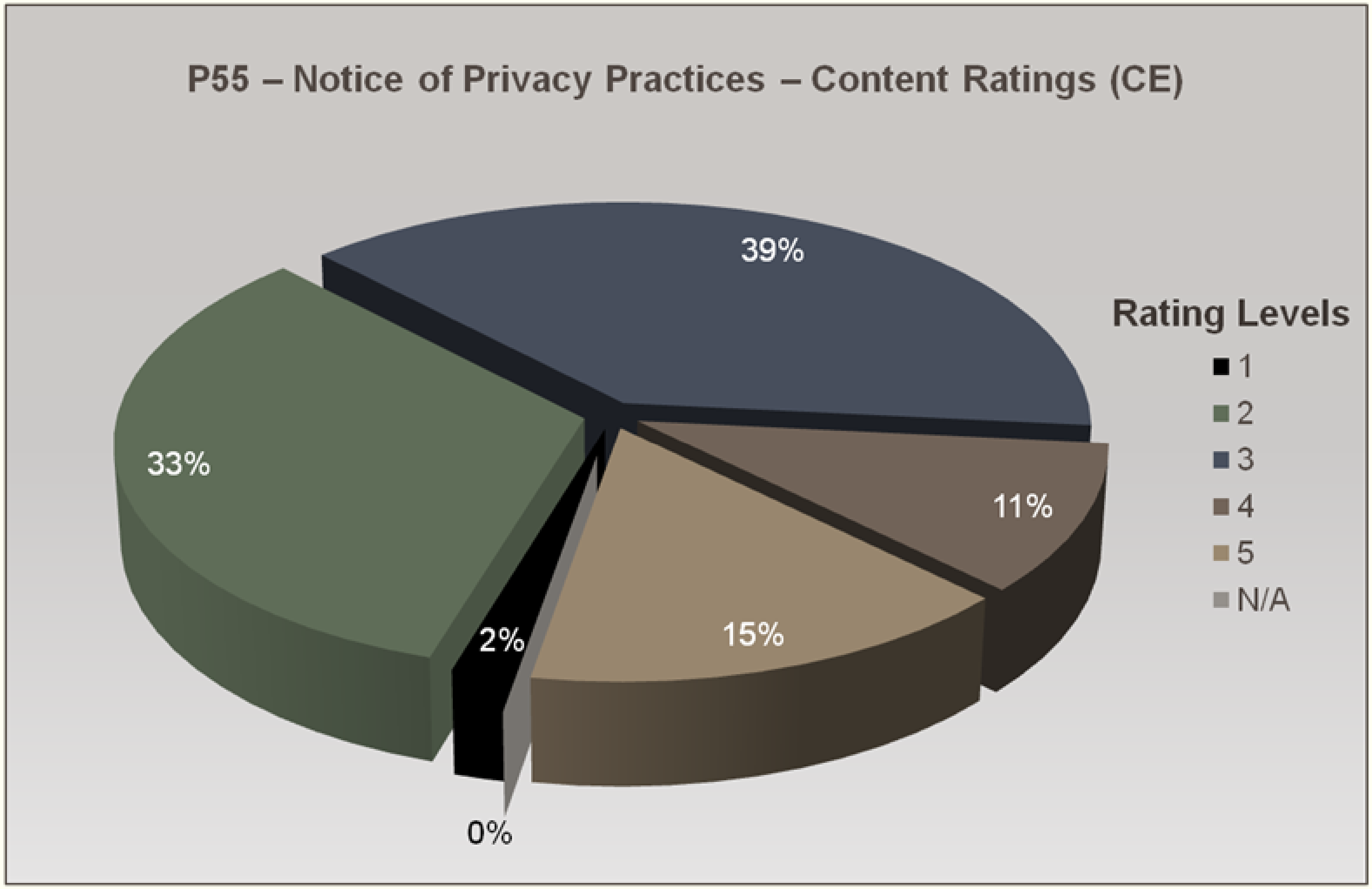
FINDINGS

CE Desk Audit Ratings

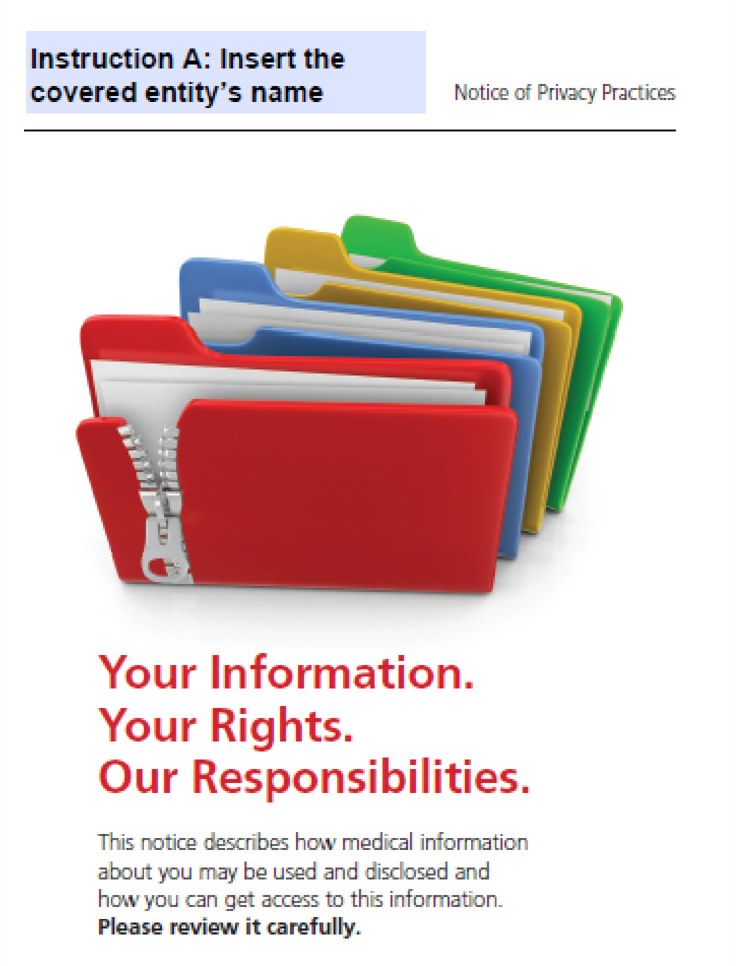


		Rating					
Element #	Provision	1	2	3	4	5	N/A
P55	Notice	2	34	40	11	16	0
P58	eNotice	59	16	4	6	15	3
P65	Access	1	10	27	54	11	0
BNR 12	Timeliness	67	6	2	9	12	7
BNR13	Content	14	15	24	38	7	5
S2	Risk Analysis	0	9	20	21	13	0
S3	Risk Management	2	2	15	28	16	0

CE Notice Content Ratings



Notices of Privacy Practices



Instruction A: Insert the covered entity's name

Notice of Privacy Practices

Your Information.
Your Rights.
Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. **Please review it carefully.**

OCR Assistance On-line

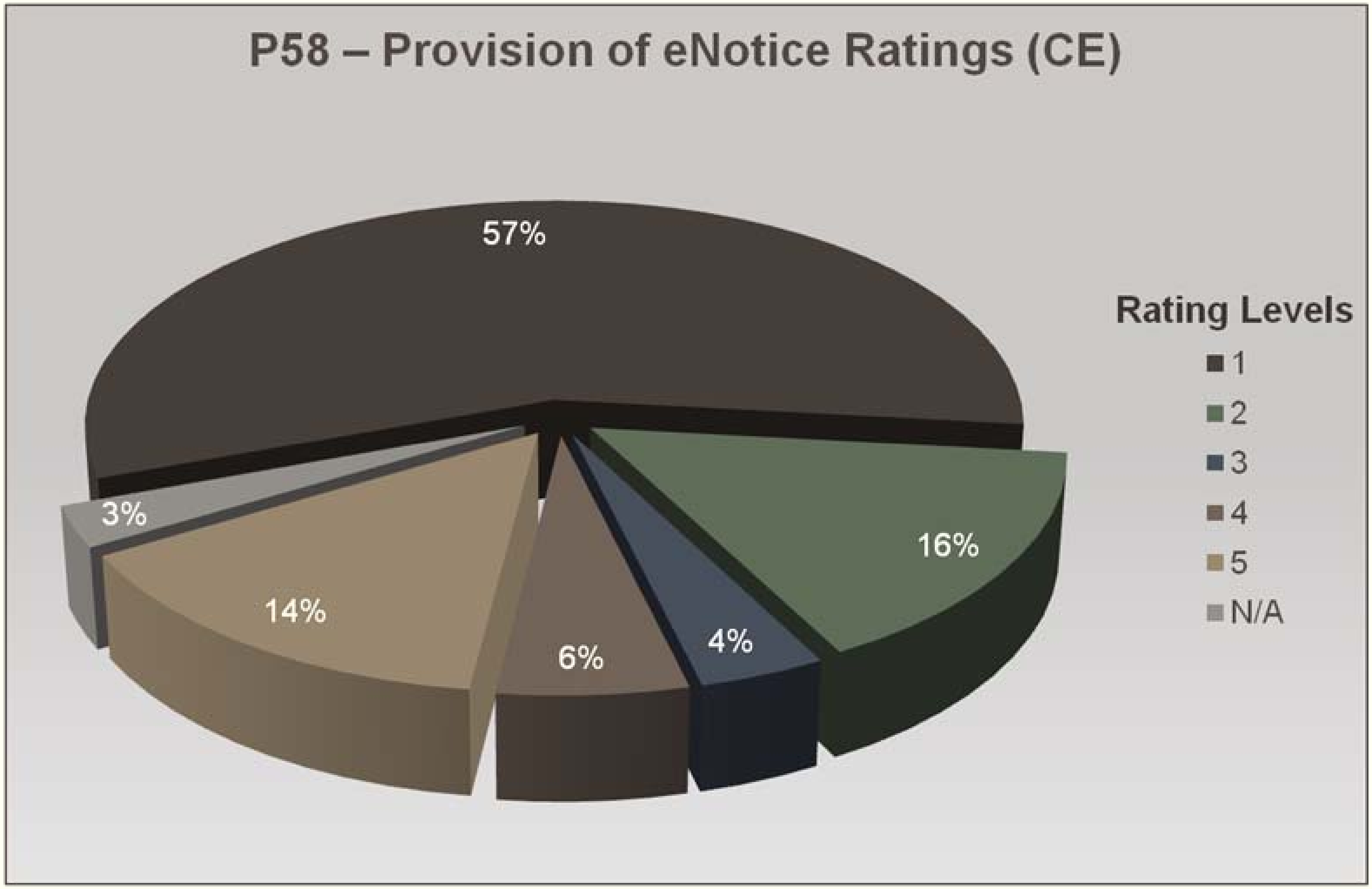
Notice of Privacy Practices for Protected Health Information

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/privacy-practices-for-protected-health-information/index.html

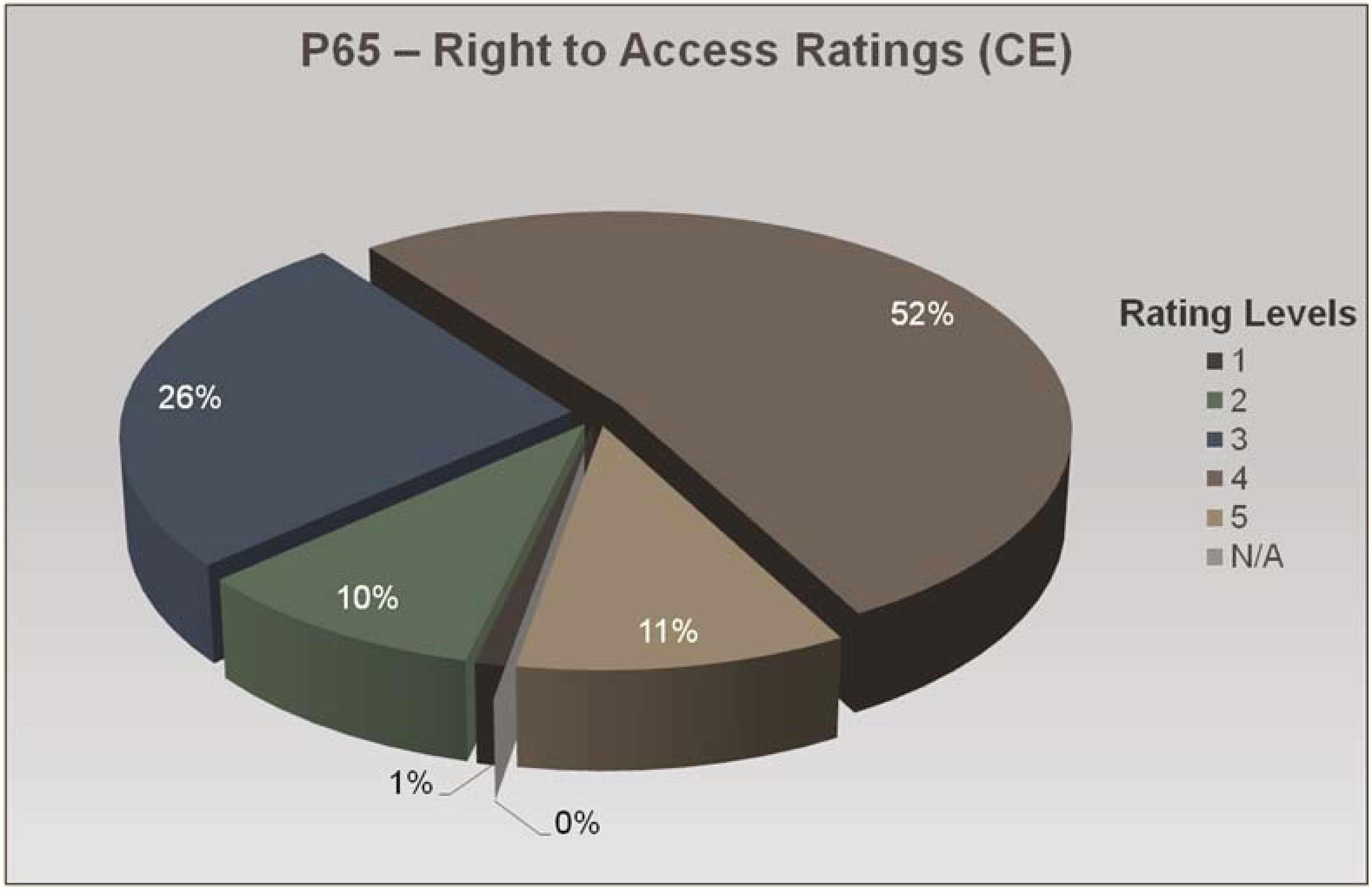
Model Notices

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html

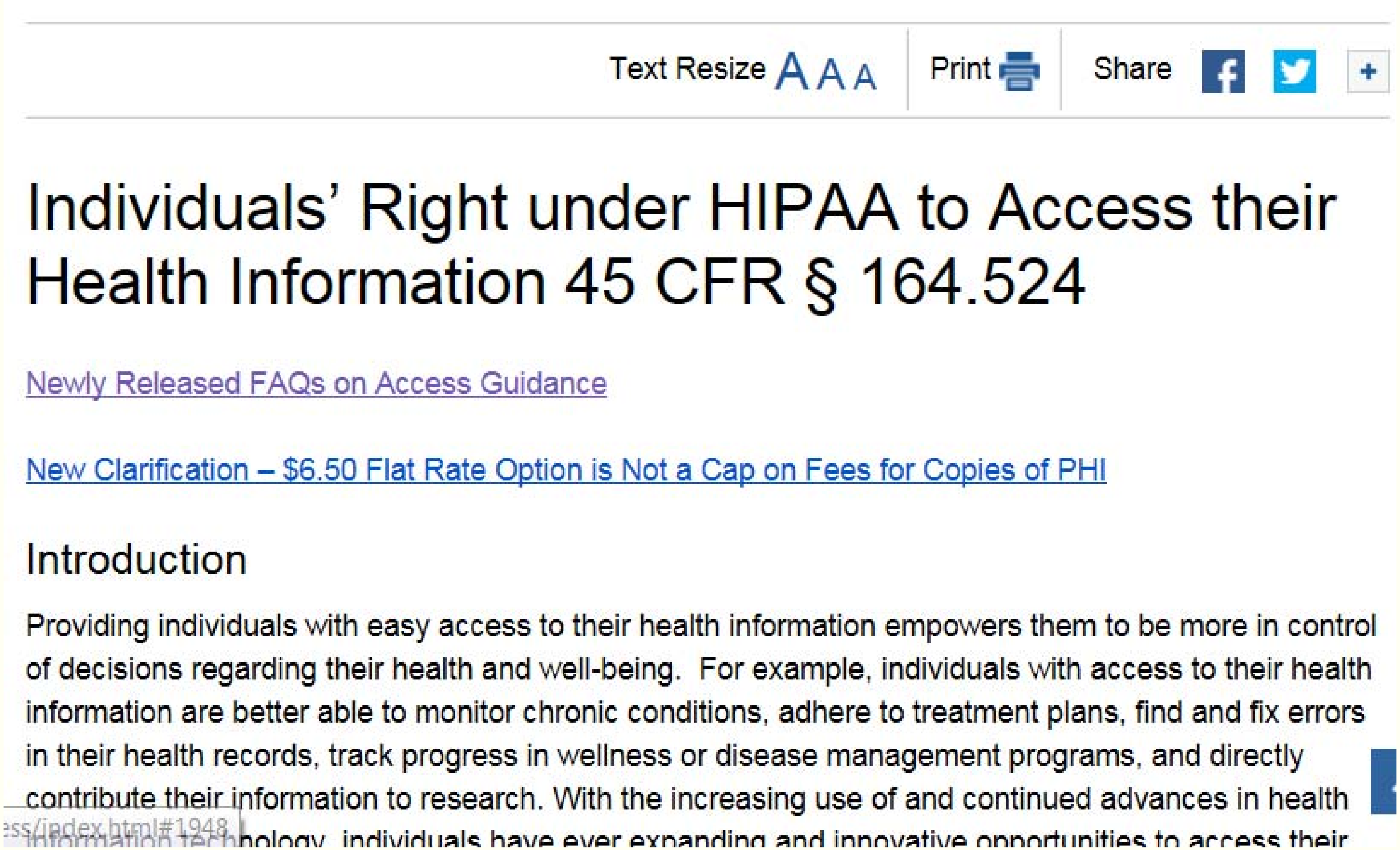
CE Notice Web Posting Ratings



CE Access Ratings



Access Resources on hhs.gov



Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

Newly Released FAQs on Access Guidance

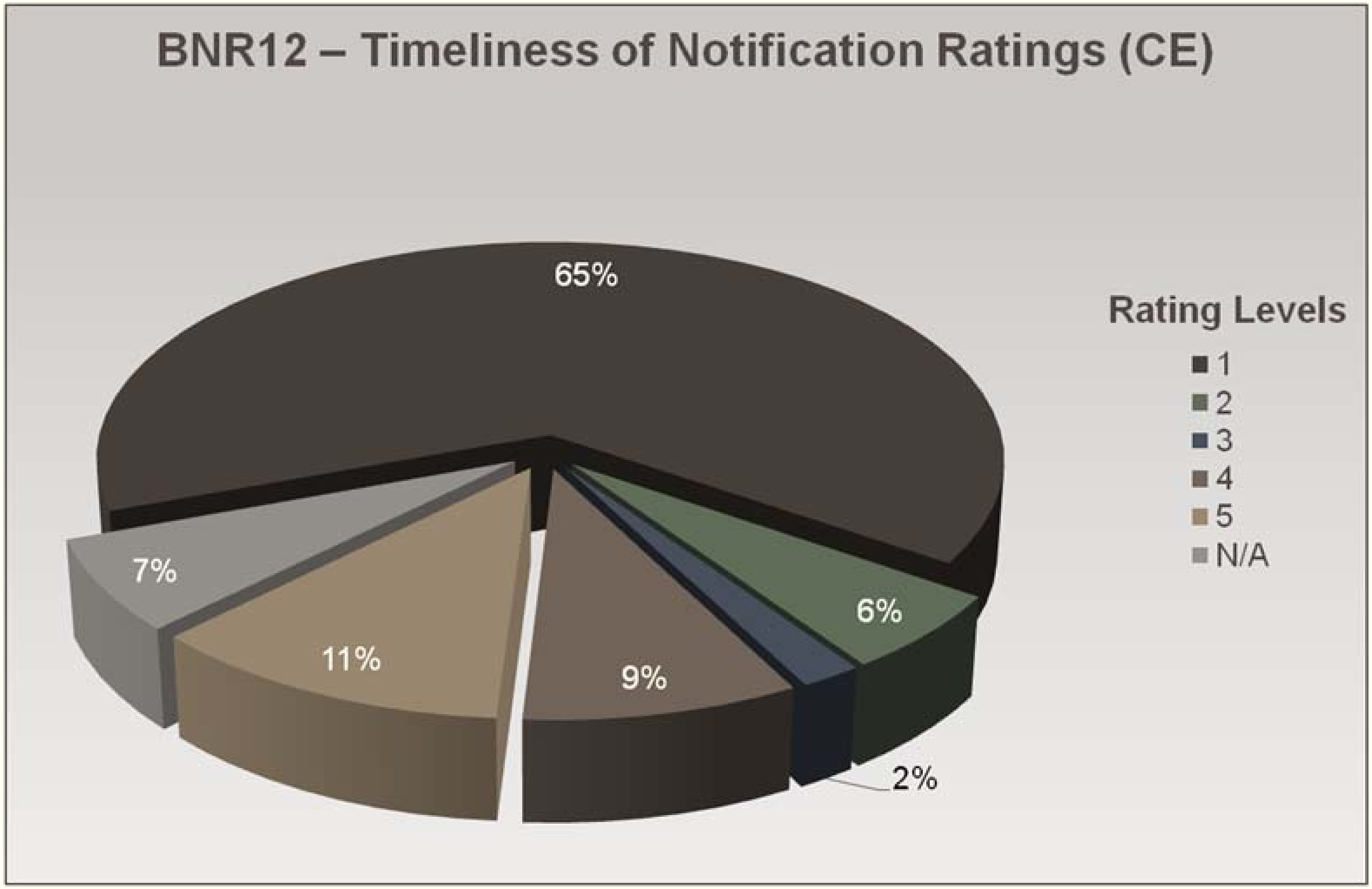
New Clarification – $6.50 Flat Rate Option is Not a Cap on Fees for Copies of PHI

Introduction

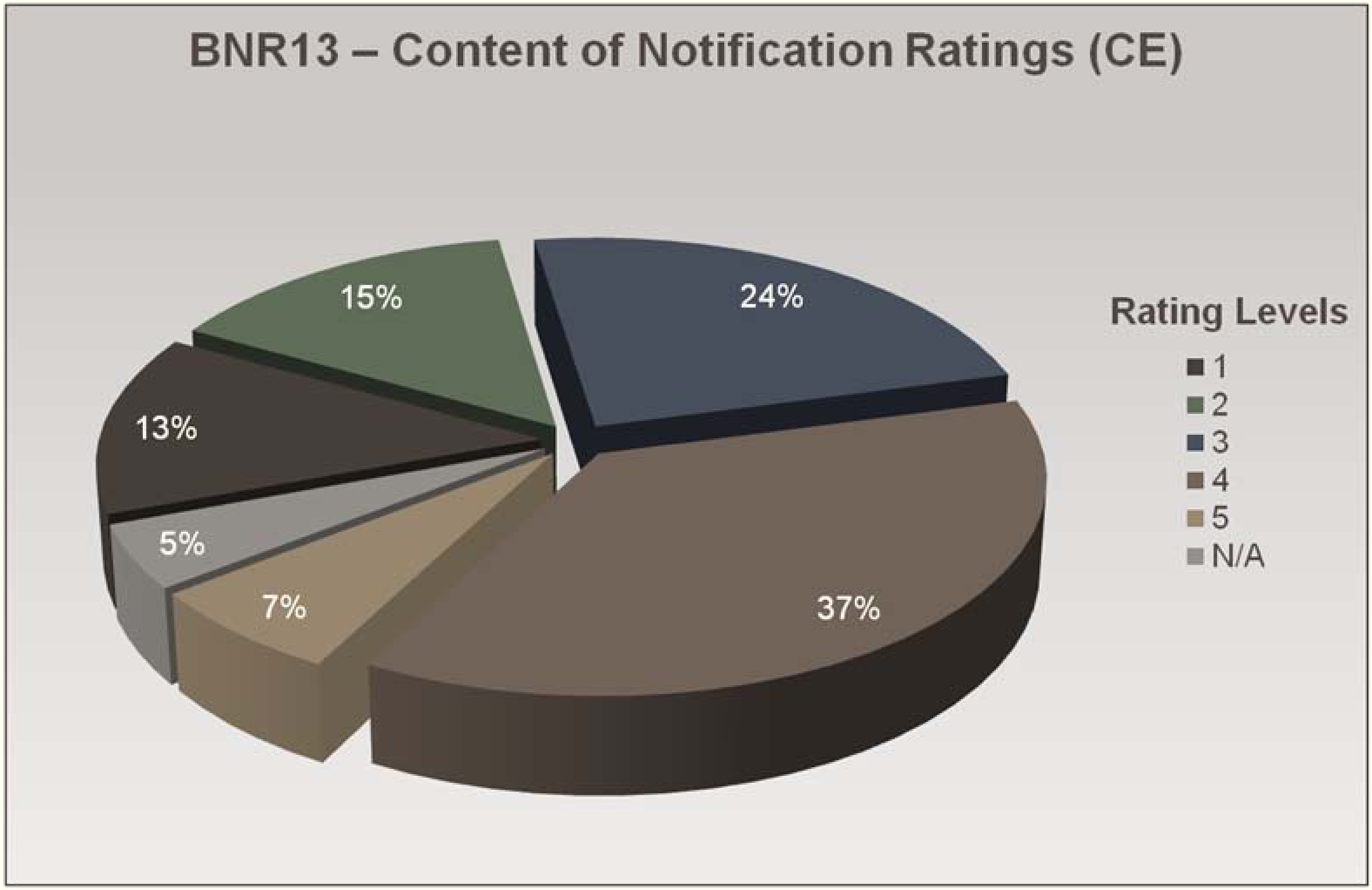
Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. With the increasing use of and continued advances in health information technology, individuals have ever expanding and innovative opportunities to access their

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

CE Breach Notification



CE Breach Notification

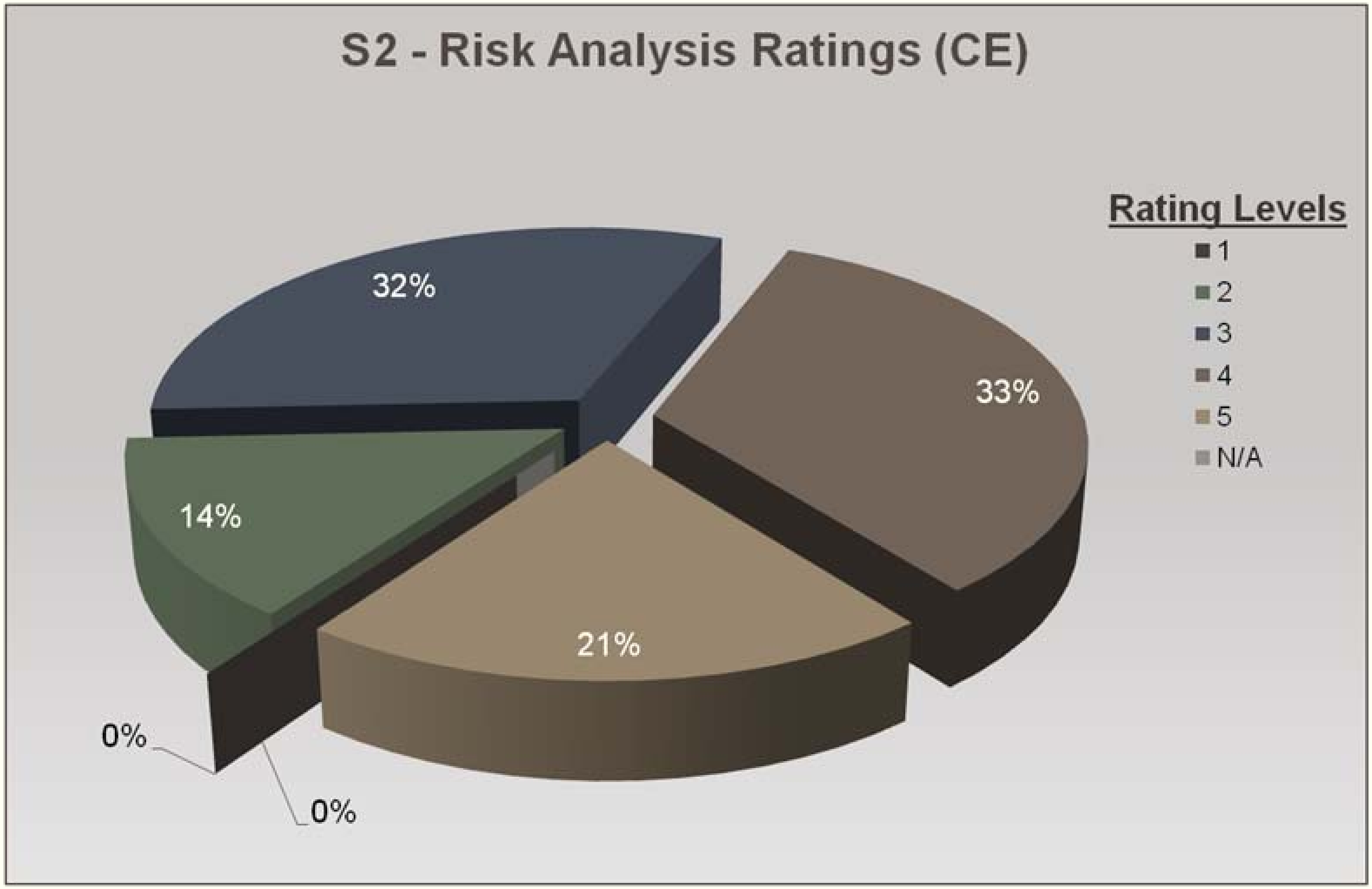


From Breach Notification Rule Guidance - CE

- Individual breach notifications must include, to the extent possible
- A brief description of the breach
- 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)

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

CE Risk Analysis Ratings



Incomplete or Inaccurate Risk Analysis

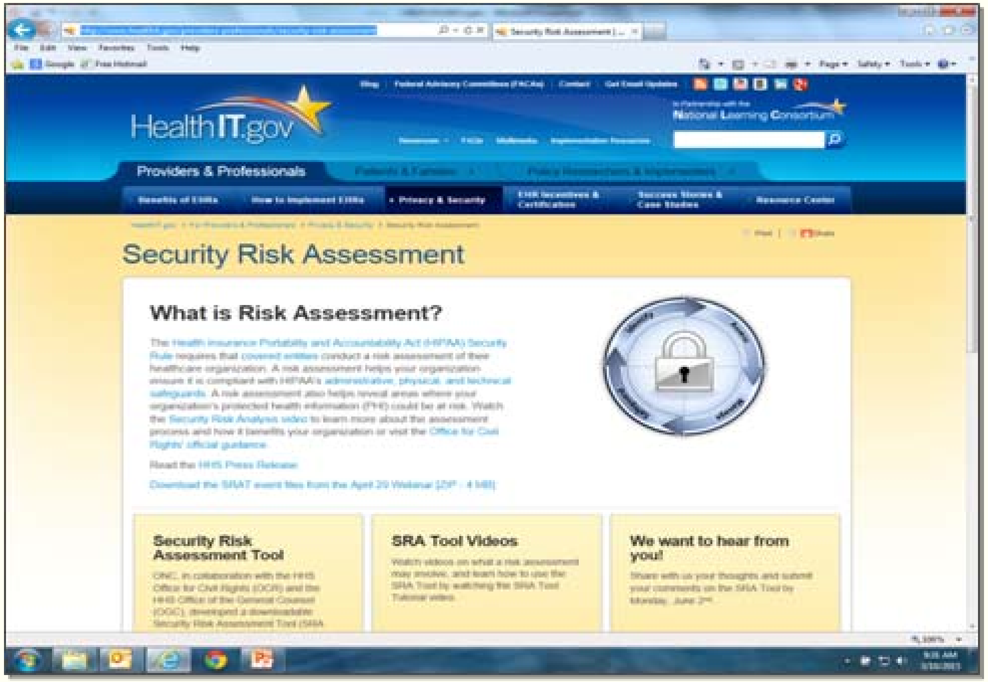
- Entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the [entity]. See 45 C.F.R. § 164.308(a)(1)(ii)(A)
- Organizations frequently underestimate the proliferation of ePHI within their environments
- Must identify all of the ePHI created, maintained, received or transmitted by the organization.
- Examples:
  - Applications like EHR, billing systems
  - Database systems and web servers
  - Fax servers, backup servers; etc.
  - Media
  - Documents and spreadsheets
  - Cloud based servers
  - Medical Devices
  - Messaging Apps (email, texting, ftp)

Risk Analysis Guidance

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

- http://scap.nist.gov/hipaa/

- http://www.healthit.gov/providers-professionals/security-risk-assessment


Blog
Federal Advisory Committees (FACAs)
Contact
Get Email Updates
HealthIT.gov
In Partnership with the National Learning Consortium
Providers & Professionals
Patients & Families
Policy Researchers & Implementers
Benefits of EHRs
How to Implement EHRs
Privacy & Security
EHR Incentives & Certification
Success Stories & Case Studies
Resource Center
Print
Share

Security Risk Assessment

What is Risk Assessment?

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. Watch the Security Risk Analysis video to learn more about the assessment process and how it benefits your organization or visit the Office for Civil Rights' official guidance.

Read the HHS Press Release

Download the SRAT event files from the April 29 Webinar [ZIP - 4 MB]

Security Risk Assessment Tool

ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable Security Risk Assessment Tool (SRA

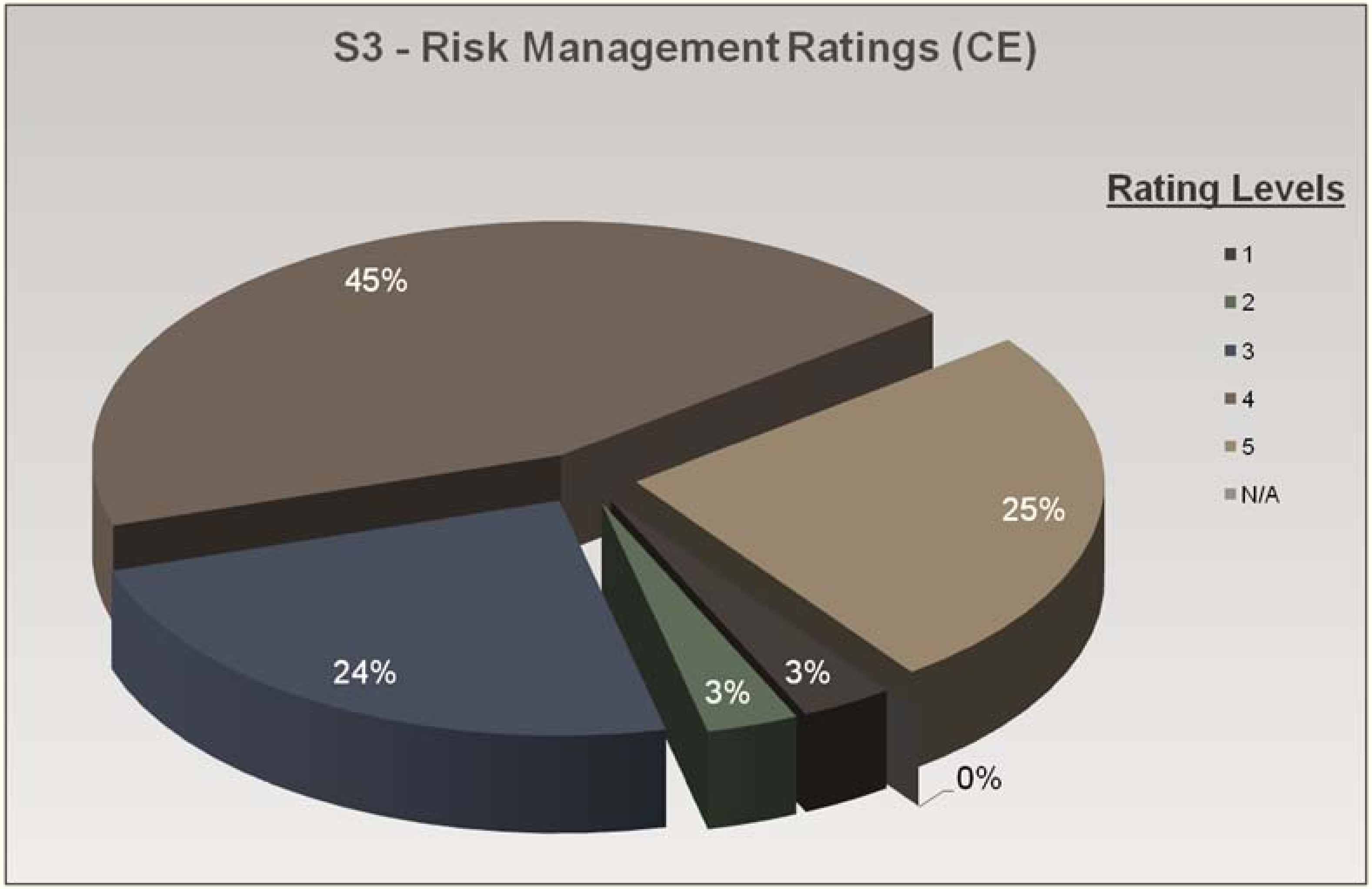
SRA Tool Videos

Watch videos on what a risk assessment may involve, and learn how to use the SRA Tool by watching the SRA Tool Tutorial video.

We want to hear from you!

Share with us your thoughts and submit your comments on the SRA Tool by Monday, June 2nd.

CE Risk Management Ratings



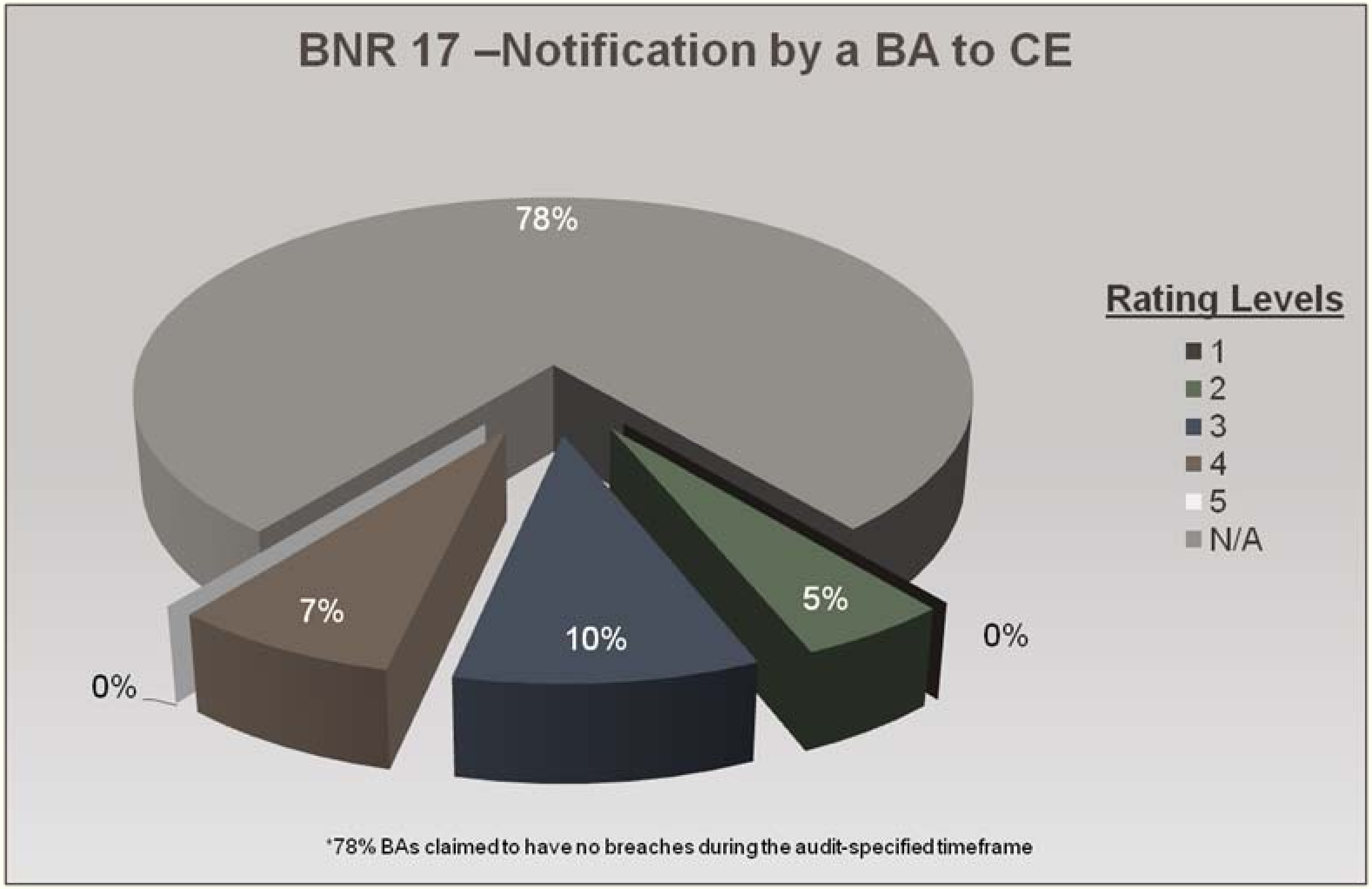
Failure to Manage Identified Risk

- The Risk Management Standard requires implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. See 45 C.F.R. § 164.308(a)(1)(ii)(B)
- OCR investigations - risks associated with reported breaches had been previously identified as part of risk analyses, but the breaching organizations failed to act on risk analyses and implement appropriate security measures
- In some instances, encryption was included as part of a remediation plan but were not carried out or were not implemented within a reasonable timeframe

BA Desk Audit Ratings

		Rating					
Element #	Provision	1	2	3	4	5	N/A
BNR17	Notice to CEs	0	2	4	3	0	32
S2	Risk Analysis	3	4	16	12	6	0
S3	Risk Management	0	5	8	21	7	0

BA Breach Notification



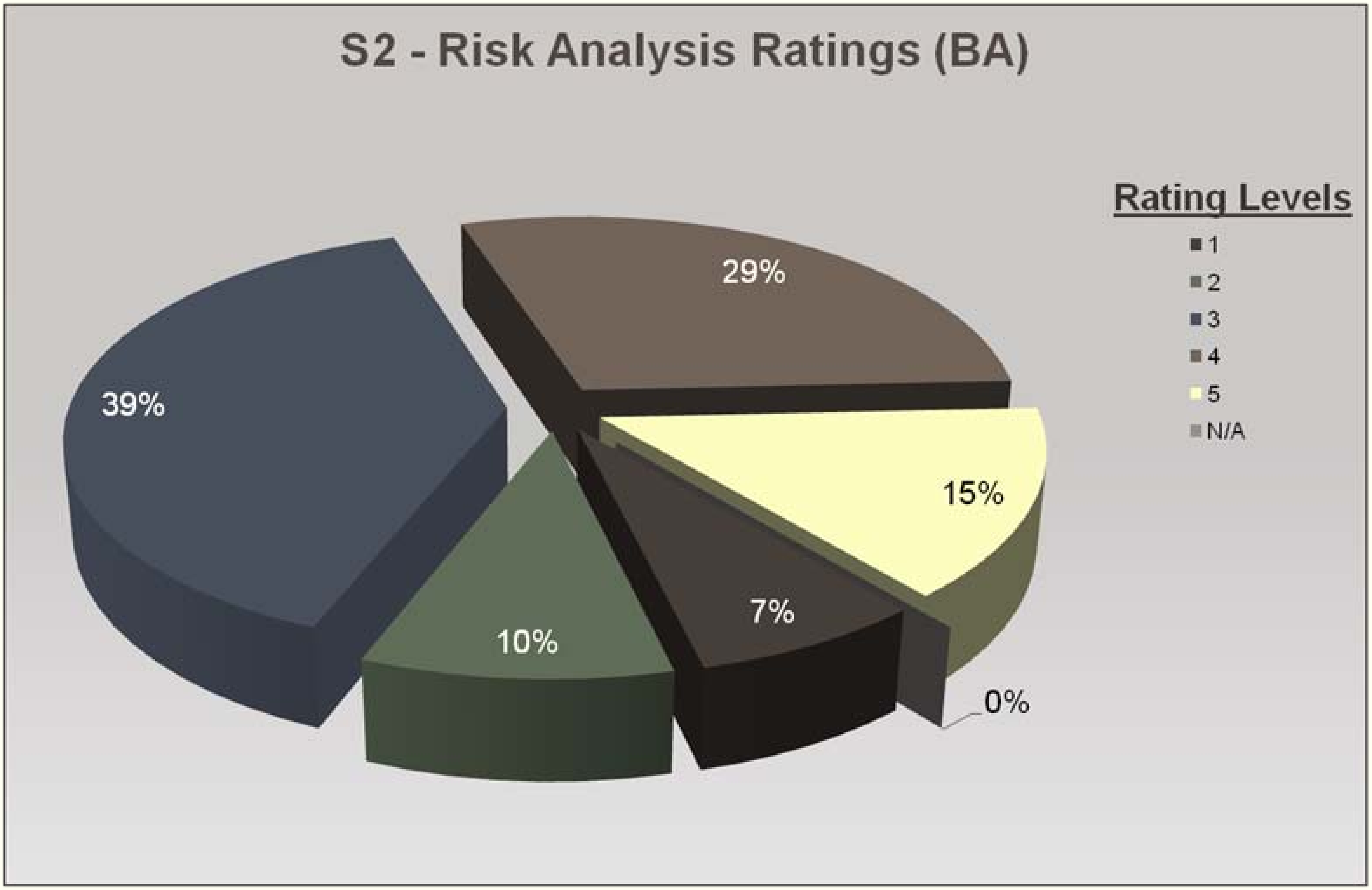
*78% BAs claimed to have no breaches during the audit-specified timeframe

From Breach Notification Rule Guidance - BA

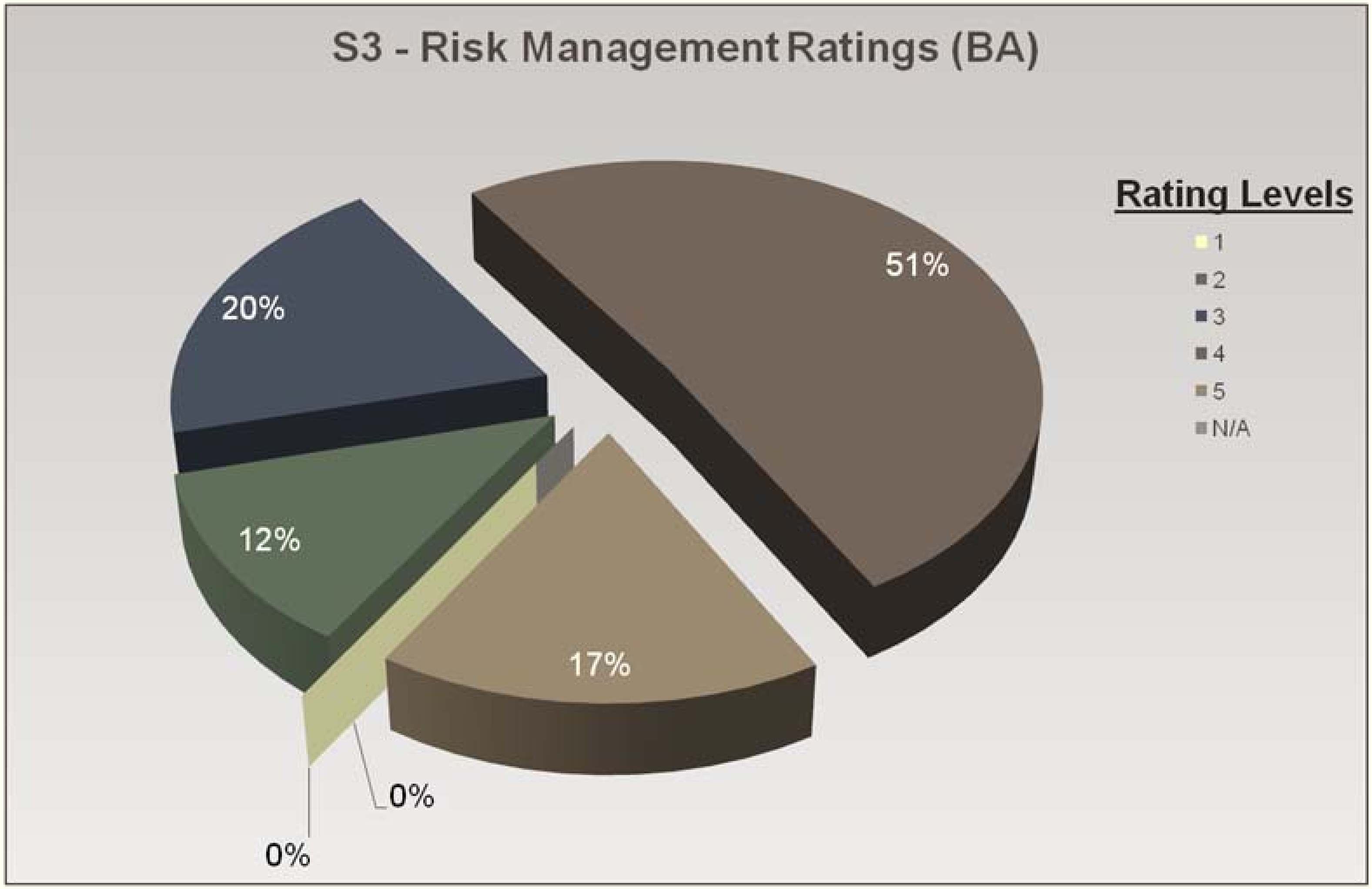
- BA must notify the CE following discovery of a breach
- BA must provide notice to the CE without unreasonable delay and no later than 60 calendar days from the discovery
- CE & BA may negotiate stricter timeframes for the BA to report
- To extent possible, BA must identify each individual affected & 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 BA, a CE may delegate the responsibility of providing the required notifications to that BA or another BA

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

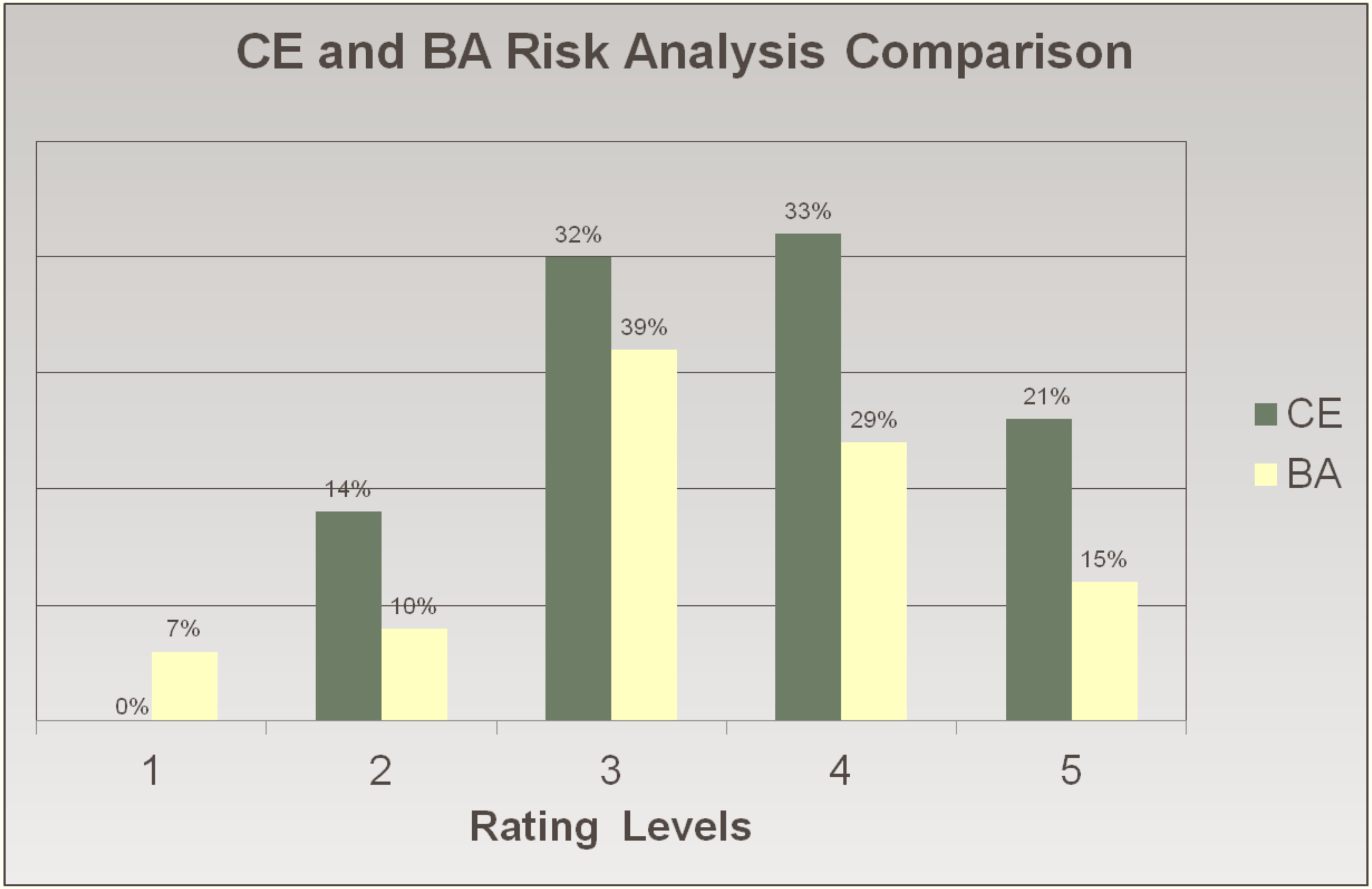
BA Risk Analysis Ratings



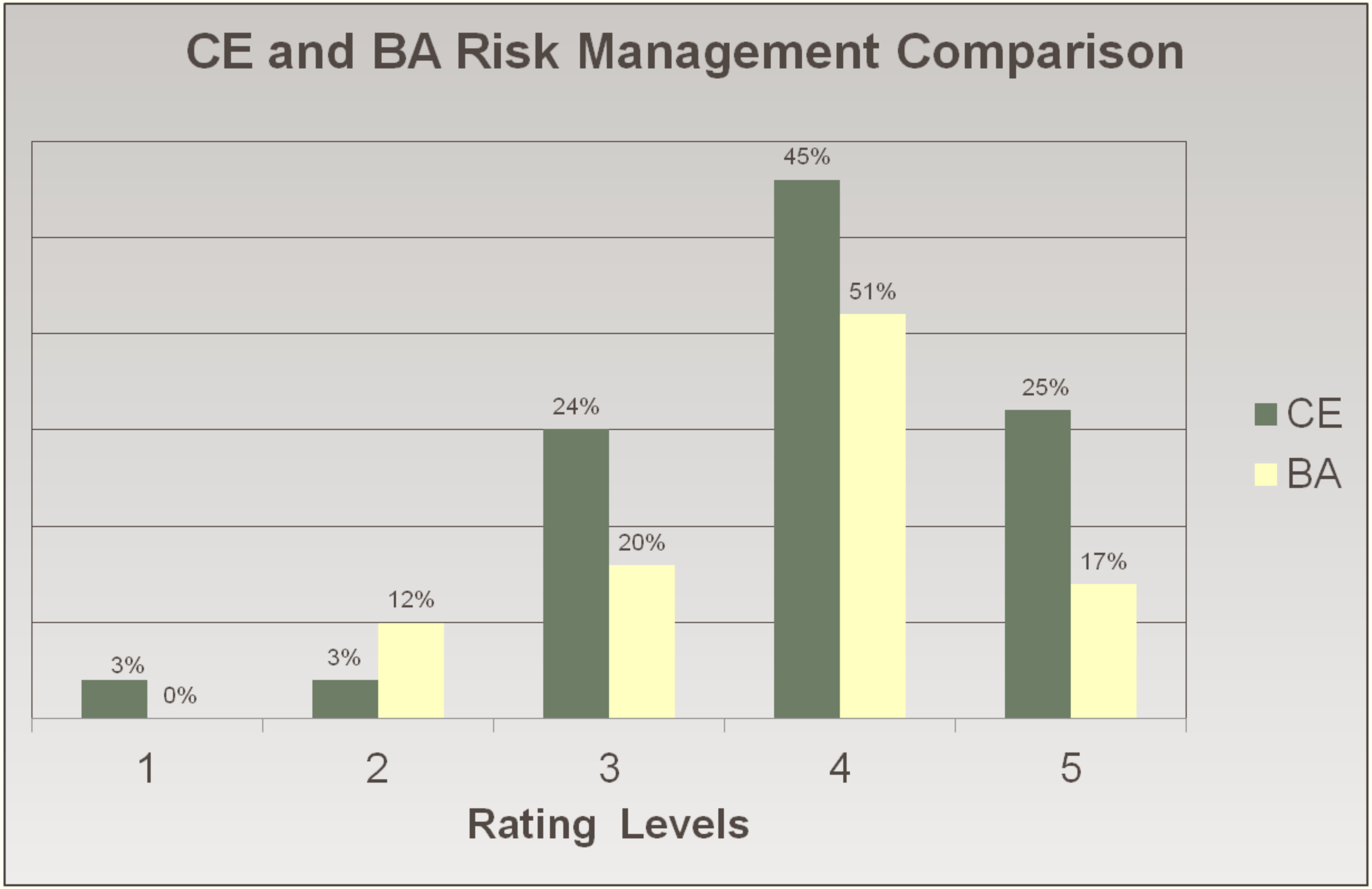
BA Risk Management Ratings



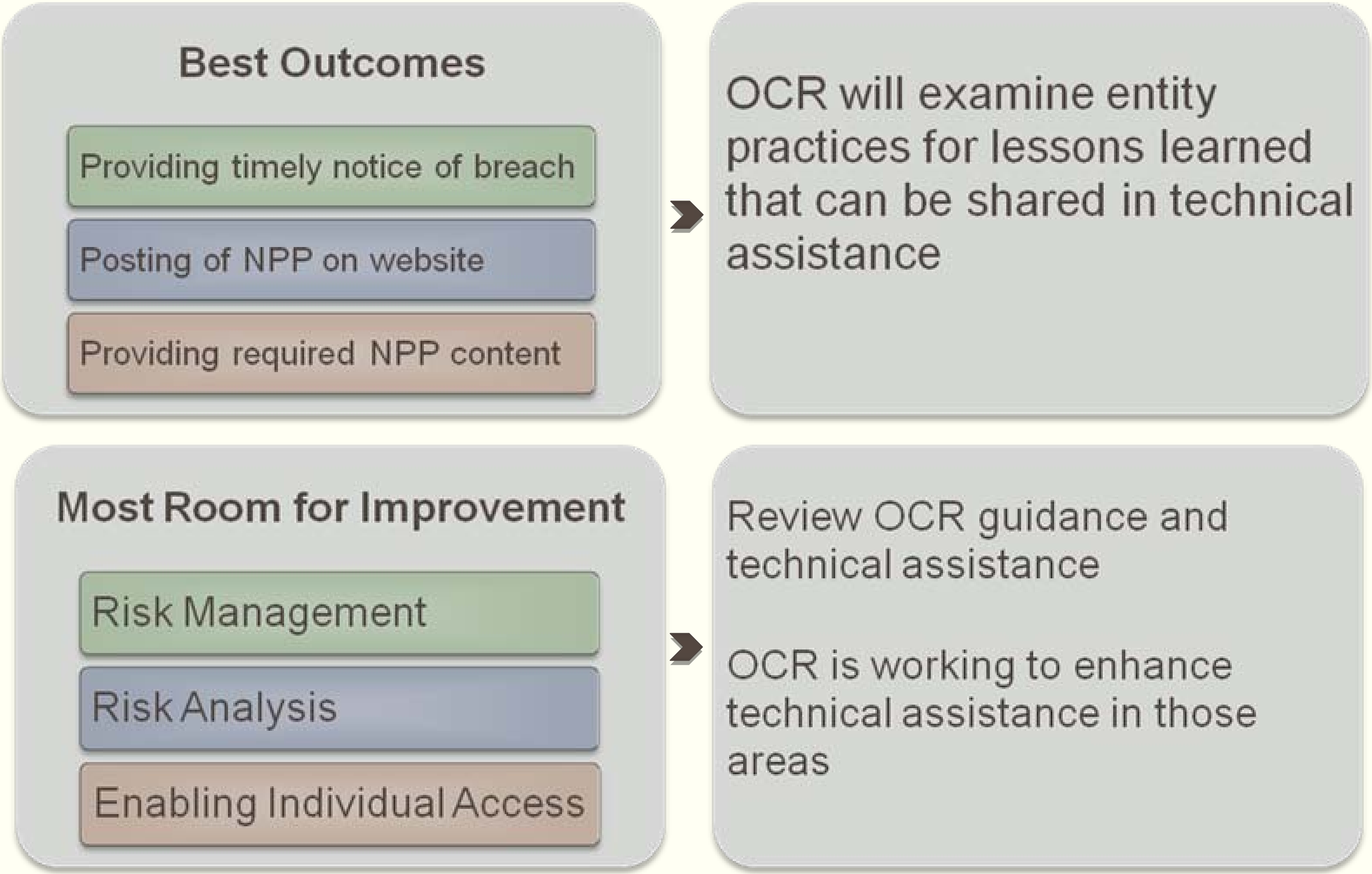
Risk Analysis Comparison



Risk Management Comparison



Industry Take-Away



Best Outcomes

- Providing timely notice of breach
- Posting of NPP on website
- Providing required NPP content

OCR will examine entity practices for lessons learned that can be shared in technical assistance

Most Room for Improvement

- Risk Management
- Risk Analysis
- Enabling Individual Access

Review OCR guidance and technical assistance

OCR is working to enhance technical assistance in those areas

More Information

- http://www.hhs.gov/hipaa

- Join us on 🐦 @hhsocr

- OSOCRAudit@hhs.gov

Lessons Learned from OCR HIPAA Audits

The 27th National HIPAA Summit

Adam Greene, JD, MPH, Partner, Davis Wright Tremaine

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Notice of Privacy Practices

- OCR is focused on right of access, including details such as:
  - Timing requirements
  - The right to an electronic copy
  - The right to have a copy forwarded to a third party
- Having a link in small font in your footer may not suffice.

Right of Access

- Important to keep policy up to date (e.g., changes governing CLIA laboratories)
- Should address permissible charges to patients

Risk Analysis

- For policy, OCR wants more than a restatement of regulation:
  - Who will conduct it?
  - How often?
  - What will trigger changes?
  - Who will receive it?
- OCR wants enterprise-wide risk analysis that is updated as new risks arise.

Risk Management

The Risk Management Policy submitted states in the procedure section that [REDACTED] shall develop and maintain a Risk Management Program to manage risk to an acceptable level.” It is very generic and does not specify what the entity is doing to manage risk – it only mentions what it will or shall do. Based on this document review, it was determined that the entity does not have a policy regarding risk management that includes:

•How risk is managed.

•What is considered an acceptable level of risk based on management approval.

•The frequency of reviewing ongoing risks. The policy provided only states “continually” and does not mention on-going risks.

•The workforce members’ roles in risk management process.

Excerpt from OCR Security Rule Desk Audit

Risk Management

- OCR wants a policy specific to HIPAA and PHI.
- For each enterprise-wide risk analysis, OCR wants to see a directly corresponding discrete risk management plan.
- Maintain evidence of implementation.

For more information

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213