American Health Information Management Association

EXTERNAL HIPAA AUDIT READINESS TOOLKIT

AHIMA
American Health Information Management Association®

EXTERNAL HIPAA AUDIT READINESS TOOLKIT

ISBN: 9781584265740
Product code: ONB202217
AHIMA Staff:
Chelsea Brotherton, *Assistant Editor*
Pamela Woolf, *Director of Publications, AHIMA Press*
Anne Zender, *Senior Director, Periodicals*

For more information about AHIMA Press publications, including updates, visit ahima.org/publications/updates.aspx

American Health Information Management Association
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601

AHIMA.ORG

TABLE OF CONTENTS

Editor's note: Appendix A is an Excel spreadsheet not included in this PDF.

FOREWORD

The HITECH Omnibus Rule mandated that the US Department of Health and Human Services (HHS) conduct periodic audits on the privacy and security compliance of covered entities (CEs) and business associates (BAs).

The first Health Insurance Portability and Accountability Act (HIPAA) audit was actually conducted by the Office of the Inspector General (OIG) in 2008 as a result of the OIG's review of the Centers for Medicare and Medicaid Services' (CMS) oversight efforts.[1] CMS was the oversight agency for the HIPAA Security Rule until 2009 when it was transferred to the Office for Civil Rights (OCR). The second and third rounds of audits were conducted under CMS' authority through PricewaterhouseCoopers[2] in 2008 and Quality Software Services[3] in 2009, respectively. Phase 1, or round four, of the HIPAA audits was conducted in 2012 and included 115 covered entities of all types and sizes.[4]

During the OCR update session on March 21, 2016, at the 2016 HIPAA Summit in Washington, DC, Deven McGraw, OCR's deputy director of health information privacy, announced that "Phase 2" of the HIPAA audits had officially begun. The HIPAA Phase 2 Audits will include both covered entities (CEs) and business associates (BAs). They include both desk audits and on-site audits and are designed to enable OCR to examine mechanisms for compliance, identify industry best practices, discover risks and vulnerabilities that have not surfaced through enforcement activities, and get out in front of problems before they result in breaches.

This toolkit is created and designed to be a single resource to provide details about external HIPAA audits and to include government resources as well as other helpful tools to help an organization prepare for any external HIPAA audit.

AUTHORS

Barb Beckett, RHIT, CHPS

Aurae Beidler, MHA, RHIA, CHPS, CHC

Aviva Halpert, RHIA, CHPS

Nancy Davis, MS, RHIA, CHPS

Elisa Gorton, MAHSM, RHIA, CHPS, CHC

Kelly McLendon, RHIA, CHPS

Angela Rose, MHA, RHIA, CHPS, FAHIMA

Roger Shindell, MS, CHPS, CISA

DeAnn Tucker, MHA-HI, RHIA, CHPS

ACKNOWLEDGMENTS

Nicole Van Andel, MS, RHIA, CHPS

Rhonda Anderson, RHIA

Patty Buttner, RHIA, CDIP, CHDA, CCS

Norma Chitvanni, RHIT, CHPS

Beth Liette, MS, RHIA

Laurie Miller, RHIT, CCS-P

Linda Renn, RHIT, CHPS, CCS, CPC, COC, CHTS-TR

Betty Rockendorf, MS, RHIA, CHTS-IM, CHPS

Donna Rugg, RHIT, CCS

Amanda Wickard, MBA, RHIA

Holly Woemmel, MA, RHIA, CHPS

INTRODUCTION

Since the OCR announced its Phase 2 HIPAA Audit Program in March 2016, selected entities were and will continue to be audited on their compliance with either the privacy rules or the security rules. The Phase 2 HIPAA Audit Program began with HIPAA CEs receiving an acknowledgment e-mail from the OCR for validation of HIPAA contact persons. Following validation, the OCR further reached out to these CEs and requested the completion of a pre-audit questionnaire. The OCR published several communications about reviewing junk and SPAM e-mail folders to ensure receipt of all OCR communications. CEs were included in the selection pool regardless of response to the validation e-mail or pre-audit questionnaire.

OCR did a randomization of all CEs and selected 167 of them for desk audits. Selected CEs were contacted via e-mail by the OCR and asked to submit documentation via the OCR portal within 10 days of receipt of the request. The requested documentation presented several challenges for the selected CEs, including the turnaround time, requested formats, and information gathering among others.

Desk audits are just the beginning of the OCR's audit plan. On-site audits are expected to begin in 2017. CEs and BAs may be subject to both types of audits. HIPAA professionals need to ensure they are able to develop and implement regulation requirements, review existing practices, and "kick the tires" to ensure CEs continue to be HIPAA compliant.

This toolkit will enable the reader to understand the requirements for OCR HIPAA Phase 2 audits, including ongoing future audits, and offers guidance regarding audit preparation and recommended practices. This toolkit can also assist CEs and BAs in meeting requirements, ascertaining how to identify which documents contain what information (and where such documents are located), and developing documentation that may be absent from a CE's or BA's HIPAA policies and procedures.

LEGAL REQUIREMENTS

WHAT ARE HIPAA AUDITS?

HHS describes the audit program as follows:

> The audit program is an important part of OCR's overall health information privacy, security, and breach notification compliance activities. OCR uses the audit program to assess the HIPAA compliance efforts of a range of entities covered by HIPAA regulations. The audits present an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews, and enable us to get out in front of problems before they result in breaches. OCR will broadly identify best practices gleaned through the audit process and will provide guidance targeted to identified compliance challenges.[5]

The first round of audits conducted as part of the OCR's HIPAA Phase 2 audit program were desk audits that began in July 2016, with a second round to be completed on BAs. These audits examined compliance with specific requirements of the privacy, security, or breach notification rules. A third round of audits (as part of the Phase 2 program) will be conducted on site and will examine a broader scope of HIPAA requirements than those addressed via the desk audits.

PURPOSE OF HIPAA AUDITS

Section 13411 of the HITECH Act states that periodic audits shall be used to ensure that CEs and BAs are in compliance with the requirements of the HITECH Act and HIPAA rules.[6] According to the OCR, "audits were primarily a compliance improvement activity."[7] The HIPAA audits, in addition to complaint investigations and compliance reviews, are one of the tools the OCR uses to:

- Proactively assess compliance with the HIPAA privacy, security, and breach notification rules
- Identify best practices
- Identify and address risks and vulnerabilities to consumer protected health information
- Better target technical assistance and guidance to CEs and BAs
- Develop a permanent audit program

The audits also help to "enhance industry awareness of compliance obligations" through the use of the OCR audit protocol for self-evaluation of CE and BA compliance with the standards and specifications of the HIPAA rules.[8]

HITECH MANDATE

HHS-mandated HIPAA compliance audits and investigations by the OCR related to compliance with HIPAA will no longer be limited to those triggered by complaints and self-reported breaches. While the audits are not intended to be investigations, an audit could reveal a serious compliance issue that could lead to a separate enforcement investigation and potential action by the OCR. These mandatory audits are further evidence of the increased enforcement efforts of HHS.

Audits are codified in Section 13411 of the law:

> 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, (CFR 45 Part 164) as such provisions are in effect as of the date of enactment of this Act, comply with such requirements.[9]

Subpart C defines the security standards for the protection of electronic protected health information (ePHI). As related to PHI, it includes items such as:

- Access
- Administrative safeguards
- Authentication
- Availability
- Confidentiality
- Encryption
- Facility
- Information system integrity
- Malicious software
- Password
- Physical safeguards
- Security or security measures
- Security incident
- Technical safeguards
- User workstation

Subpart E defines the privacy of individually identifiable health information and includes:

- Uses and disclosures
- Notice of privacy practices
- Amendment of PHI
- Accounting for disclosures

THE OFFICE FOR CIVIL RIGHTS HIPAA AUDIT PROCESS

On July 13, 2016, the OCR conducted an informational webinar for entities chosen as part of the HIPAA Phase 2 Audit Program. Director Jocelyn Samuels emphasized that "the primary purpose of these audits is to help us all learn how we can work together to best protect the information that we hold."[10]

Most of the information below, including FAQs and the July presentation, can be found at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/.

DESK AUDITS

Selection

OCR identified pools of CEs that represented a wide range of healthcare providers, health plans, and healthcare clearinghouses to better assess HIPAA compliance across the industry. Information provided by HHS in response to the audit pre-screening questionnaire was used for the selection process. Sampling criteria included size, affiliations, location, and whether the organization was public or private. Health plans were divided into group plans and issuers. Providers were further categorized by type of healthcare facility.

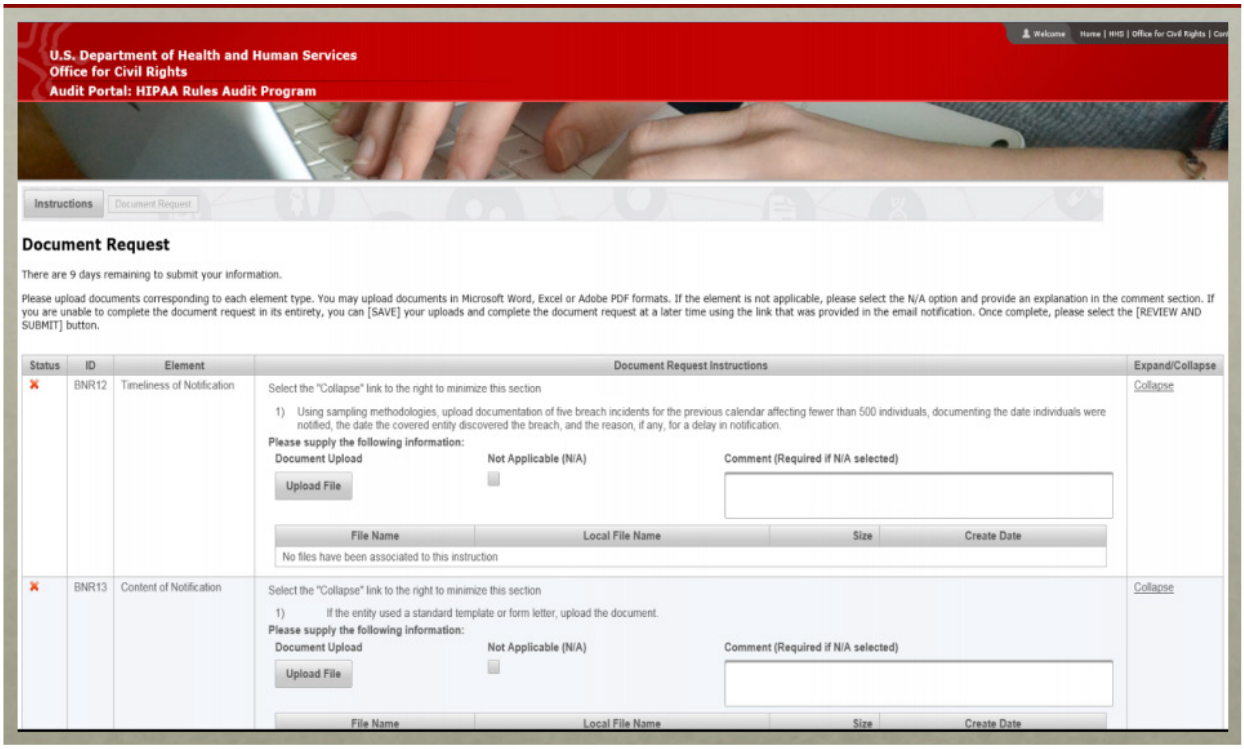
OCR then conducted a randomized selection algorithm that drew from each of the categories, resulting in 167 selected CEs. The auditees were checked for conflicts of interest with the contractor supporting OCR in the audit process as well as subjects of ongoing investigations. Conflicting auditees were replaced with new ones. CEs involved in an ongoing investigation with the OCR were not chosen. CE desk audits were expected to be conducted through the end of 2016.

Document Submission

Document request notifications were sent to selected auditees via e-mail. CEs were expected to watch their spam and junk e-mail folders for any e-mails from the OCR. Two e-mails were sent requesting information, one requesting policies, procedures, and/or other related documentation while the second requested a listing of all the CE's BAs. BA listings were requested to be submitted in an electronic format, via e-mail, to OCR within 10 business days. All other items were required to be submitted using the secure online portal link provided in the notification e-mail (see screenshot below).

The scope of the desk audits is limited to a total of seven controls drawn from the Security Rule, the Privacy Rule, and the Breach Notification Rule. Depending upon the type of entity, each auditee was expected to provide only the policies and procedures relevant to the controls requested. Auditees were responsible for providing clear, complete, and responsive documentation to OCR. CEs were warned that they would not receive "credit" for late document submissions. If a CE did not have the requested documentation, it was instructed to submit an explanation for the deficiency.

OFFICE FOR CIVIL RIGHTS DOCUMENT SUBMISSION PORTAL



Source: Samuels, Jocelyn, et al. "HIPAA Privacy, Security & Breach Notification Compliance Audits Phase 2." Webinar, July 13, 2016.

ON-SITE AUDITS

On-site audits will begin in 2017, evaluating auditees against a comprehensive set of HIPAA compliance controls. A desk auditee may also be subject to an on-site audit; being selected for a desk audit does not remove the CE from the selection pool for the on-site audits. CEs can be selected for a desk audit, an on-site audit, or both, according to Samuels' presentation.

CEs will also be notified by e-mail of selection for an on-site audit. Auditors will schedule an entrance conference and provide the details and expectations of the on-site audit process. Based on the size of the entity, each on-site audit will be conducted over three to five days. On-site audits will be more comprehensive than desk audits and cover a wider range of requirements from the HIPAA rules.

FINDINGS: DESK AND ON-SITE AUDITS

Draft findings will be provided to auditees upon completion of the audits. Auditees will have 10 business days to respond with comments. A final report from the auditor will be provided to the CE and any selected BAs 30 business days from the auditee's response.[11]

BUSINESS ASSOCIATE AUDITS

The HIPAA Phase 2 audits will be the first time that BAs will be audited for compliance with HIPAA. OCR announced in September 2016 that the 40 to 50 BAs selected for an audit will be notified in October 2016. The BA auditee selection pool was built from the list of BAs requested by each CE that received a desk audit. BAs will have the same expectations and follow the same process as CEs for desk audits and on-site audits.

SECTION III: HIPAA AUDIT PREPARATION

OCR has created several tools, including the HIPAA Audit Protocol (http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/), to assist CEs and BAs in preparing for an audit. The CE or BA will want to review the protocol and identify gaps in meeting the established performance criteria. Appendix A provides an overview of the OCR's HIPAA Audit Protocol including summaries and Appendix B provides a sample document request checklist.

While the Audit Protocol is a useful tool in assessing the CE's or BA's status, it is not an overall privacy and security compliance plan and focuses only on the OCR's requirements. It is recommended that the CE and BA have in place its own HIPAA privacy and security rule compliance plan and/or policy (refer to Appendix C) that is not only meaningful for the organization, but meets the needs of other external review organizations such as licensing bodies and accrediting agencies as well as supporting documentation for legal proceedings.

The CE or BA will want to take steps in advance to demonstrate ongoing compliance with the HIPAA privacy and security rules. The age-old adage "if you didn't write it down, it didn't happen" applies to HIPAA privacy and security processes as well as other healthcare operations. It is advisable for the CE and BA to organize the elements of its HIPAA compliance efforts in a centralized manner where supporting documentation is easily accessible to respond to any external audit of privacy and security practices.

The CE or BA may want to consider creating a "HIPAA Compliance Plan" to centralize the supporting documentation for HIPAA audit readiness and review the plan annually. Completion of the plan will help the CE and BA in responding to protocol criteria as well. Whether a plan is created or not, the CE or BA will want to ensure that the following elements are addressed in its HIPAA compliance efforts:

PRIVACY OFFICER JOB DESCRIPTION

Not only is the organization required to designate a privacy officer, the role should be outlined in a formal job description with the scope of duties delineated. Refer to Appendix D for a sample job description.

HIPAA OVERSIGHT COMMITTEE

If an oversight committee exists or HIPAA compliance activities are integrated into an overall compliance committee, a description of the committee and even its charter is helpful in demonstrating a commitment to HIPAA compliance. Charter elements may include:

- Name of oversight committee
- Description/scope
- Date established
- Members and member responsibilities
- Reporting structure
- Facilitator
- Maintenance of agendas and minutes
- Schedule
- Resources required
- Deliverables

The availability of documented meeting minutes will demonstrate the CE's and BA's long-term commitment to compliance.

POLICIES AND PROCEDURES

At a minimum, the CE or BA will want to ensure the establishment of HIPAA privacy and security policies that address key patient rights as well as other administrative, technical, and physical safeguards. Refer to Appendix E and Appendix F for a sample list of policies, procedures, and forms that should be created and implemented to ensure success in meeting HIPAA compliance.

It is critical that policies illustrate dates created, expiration, or revision dates as well as review dates and any actions taken. CEs and BAs should maintain copies of prior/old policies and procedures. It is recommended that the CE be able to easily generate a policy log that delineates a listing of privacy and security policies with the following elements:

- Number/title of policy
- Date established
- Review dates

TRAINING, EDUCATION, AND AWARENESS ACTIVITIES

The CE and BA should have available an inventory of training, education, and awareness activities that includes, at a minimum, new employee orientation and any mandatory education activities. It is advisable for the CE and BA to keep a listing of all privacy and security training, education, and awareness activities including newsletter articles, focused training, presentations, tools, frequently asked question documents, etc. Such an inventory of activities, dates, and audiences will also demonstrate ongoing compliance. The CE and BA should be able to produce the information provided in its training, education, and awareness activities upon request of an external auditor.

METRICS

The CE and BA should have in place key metrics used for reporting compliance activities to leadership. Metrics may include, but are not be limited to:

- Number of privacy investigations
- Number of reportable breaches
- Reportable breach rate
- OCR investigations/letters (external)
- Number of EHR access audits carried out
- Number of positive EHR access audits (breaches)
- Number of helpline calls
- Number of identity theft/misrepresentations

The ability to produce data on sustained monitoring of key metrics will support HIPAA audit readiness.

ELECTRONIC HEALTH RECORD (EHR) ACCESS AUDIT PLAN

If the CE utilizes an EHR, there should be in place a plan to indicate the scope of access auditing as well as frequency and the management of audit results. See Appendix G for a sample access audit plan.

LEADERSHIP REPORTING TOOLS

Activities related to HIPAA compliance should be reported on a regular basis to CE and BA leadership, including the board of directors. At a minimum, this reporting should occur annually and copies of these reports integrated into the overall HIPAA compliance documentation. Refer to Appendix H for a sample reporting dashboard.

The CE's or BA's HIPAA compliance activities may be tested through external audits for meaningful use or general vendor-based audits for privacy and security. Additionally, the CE or BA can explore creating an internal "mock" audit to be carried out across the organization. Mock audits can encompass the OCR protocol, training activities, and privacy and security rounds addressing key elements. Any form of audit compliance activities will identify strengths and opportunities for improvement.

SECTION IV: THE FUTURE OF HIPAA AUDITS

There is no way to know exactly what the future holds for any auditing process. It is evident, however, that audits will continue to occur in one form or another. With the ever-evolving and improving technology that stores, maintains, and transmits PHI, auditing functions will increase.

HIM and privacy staff are becoming "investigators," constantly monitoring data access, disclosure, and usage, as well as proactively auditing compliance with regulations and policy, such as walk-through physical monitoring (i.e., privacy rounds, security rounds). Regulatory and legal actions continuously change, so a strong auditing and monitoring program can help minimize legal interventions and possible sanctions. New areas of possible focus beginning to appear include user access audits for disgruntled employees, terminated employees (i.e., others accessing that PHI), management/executive/board members, noteworthy/high-profile accounts, random patient accounts, and employee patients.

The waters are being tested both by the government and by patients as new guidelines evolve outlining protocols, expectations, and requirements. The privacy, compliance, HIM, and IT/IS departments must work collaboratively to be prepared, closely monitoring compliance with regulations, protocols, and policies of the CE or BA. The need for more staff to function as auditors/monitors and analysts for privacy and security is growing at an ever-increasing speed. Policies will need to be revised routinely and compliance regularly monitored.

There will be challenges encountered along the audit path. CEs and BAs must continually update programs to provide a multitude of auditing opportunities. Will programs provide the auditing ability needed for a high level of compliance? Keeping abreast of all federal and state regulations and protocols and having access to the latest information is paramount for optimal outcomes.

Notes

1. Rose, Angela Dinh. "What to Expect When Phase 2 HIPAA Audits Begin." *Journal of AHIMA* 87, no.6 (June 2016): 34-35.

2. Ibid.

3. Ibid.

4. Ibid.

5. US Department of Health and Human Services. "HIPAA Privacy, Security, and Breach Notification Audit Program." http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/#when.

6. American Recovery and Reinvestment Act of 2009, Public Law 111–5, 111th Congress, 1st session (Feb. 17, 2009). http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

7. US Department of Health and Human Services. "Audit Pilot Program." http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/pilot-program/index.html.

8. Ibid.

9. American Recovery and Reinvestment Act of 2009.

10. Samuels, Jocelyn, et al. "HIPAA Privacy, Security & Breach Notification Compliance Audits Phase 2." Webinar, July 13, 2016. http://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf.

11. Rose, Angela Dinh. "What to Expect When Phase 2 HIPAA Audits Begin."

SECTION V: APPENDICES

APPENDIX A
HIPAA AUDIT PROTOCOLS SUMMARIES AND CHECKLIST

Editor's note: Appendix A is an Excel spreadsheet not included in this PDF.

APPENDIX B

POTENTIAL OCR AUDIT DOCUMENT REQUEST LIST (2016)

Note: This information is for reference purposes only.

Authors' note: This list is created from the actual language of the OCR breach protocols and has been edited and rendered more readable. The intent was to capture all of the possible requests generated by action verbs within the OCR "Audit Inquiry" column within the protocol line items, at least in a somewhat summarized form. The intent is to have generated an easily usable list. Please note that OCR may ask for documents in a slightly different manner than listed here. **Items in bold type represent actual OCR audit documents that were requested from auditees for the desk audits in summer 2016.**

The number at the end of each line item (e.g., (BNR16)) corresponds to the OCR protocols numbers (the prefixes - BNR=Breach Rule, P=Privacy Rule, and S=Security Rule). If multiple numbers appear (e.g., (BNR1) (BNR7) (BNR7) (BNR9)(BNR12)), this indicates a line item that is repeated and addressed within multiple protocols.

APPENDIX B1

BREACH AUDIT REQUEST DOCUMENTS

1. Policies(s) and procedure(s) (P&P) related to breach, including language regarding training; complaints to covered entity (CE); sanctions; refraining from retaliatory acts; waiver of rights and documentation; notification (individuals and media); and other areas (BNR1) (BNR7)(BNR12) (BNR13) (BNR14) (BNR15) (BNR16) (BNR16) (BNR18)
2. Copy of the content of training (BNR2)
3. Evidence of training (e.g., sign-in sheets) (BNR2)
4. Breach complaint process in place (BNR3)
5. List of complaints received in the specified period and the disposition of such complaints (BNR3)
6. Use sampling methodologies to select complaints to be reviewed (BNR3)
7. Documentation of actions taken by the CE or business associate (BA) to investigate and resolve the potential breach (BNR3)
8. List of sanctions; include type of action led to sanction and other relevant info (BNR4)
9. Use sampling methods to choose sanctions to be reviewed (BNR4)
10. P&P related to refraining from retaliatory acts (BNR5)
11. Obtain any patient or health plan member intake forms to ensure they contain waiver of rights language (BNR6)
12. P&P for requiring BA to report an impermissible use or disclosure of protected health information (PHI) to the CE and the CE's process for handling such reports (BNR7)
13. Documentation that the CE maintains its P&P, in written or electronic form, until six years after the later of the date of their creation or the last effective date (BNR8)
14. Documentation that the CE maintains all other documentation required by 164.530(j)(1) until six years after the later of the date of their creation or the last effective date (BNR8)
15. Process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised (BNR9)
16. If there's not a process for breach assessment, does the CE have a P&P that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI (BNR9)
17. Review the CE's risk assessment P&P, if the CE does not have a P&P that treats all potential breaches as requiring notifications without conducting a risk assessment (BNR9)
18. List of risk assessments, if any, conducted within the specified period where the CE determined there was a low probability of compromise to the PHI (BNR9)
19. Use sampling methodologies to select documentation of risk assessments (BNR9)
20. List of risk assessments, if any, conducted within the specified period where the covered entity determined that the PHI was compromised and notification (BNR9) rendered
21. Use sampling methodologies to select documentation of risk assessments (BNR9)
22. Documentation of a determine that one of the regulatory exceptions to the definition of breach at §164.402(1) applies (to a potential breach), if any (BNR10)

23. Use sampling methodologies to select and review documentation of one of the regulatory exceptions to the definition of breach (BNR10)
24. Obtain documentation where a CE or BA determined that the violation did not require notification, because the PHI was not unsecured PHI (BNR10) and therefore not a breach
25. Use sampling methodologies to select and review documentation determining that the breach did not require notification, because the PHI was not unsecured PHI (BNR10)
26. **Question from July 2016 audit: Upload documentation of five breach incidents for the previous calendar year 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 (BNR12)(BNR16)**
27. **Question from July 2016 audit: If the entity used a standard template or form letter, upload the document (BNR13)**
28. Obtain a list of breaches, if any, in the specified period and documentation indicating (BNR12)
29. **Question from July 2016 audit: upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year (BNR13)(BNR15)(BRN16)**
30. **Question from July 2016 audit: Upload a copy of a single written notice sent to affected individuals for each breach incident (BNR13)**
31. List of breaches, if any, in the specified period and documentation of written notices sent to affected individuals for each breach (BNR13)
32. Use sampling methodologies to select notifications sent to individuals to be reviewed (BNR13)
33. Documentation of any breaches within the specified period that required substitute notice (BNR14)
34. Documentation of a conspicuous posting on the home page of the covered entity's web site or a copy of conspicuous notices in major print or broadcast media and documentation of a toll-free phone number that remained active for at least 90 days (BNR14)
35. Use sampling methodologies to select notifications to be reviewed (BNR14)
36. Documentation to verify that the media notifications included the elements required (BNR15)
37. Documentation of notifications provided to the Secretary (BNR16)
38. Sampling methodologies to select notifications to be reviewed (BNR16)
39. Documentation of notifications provided to the Secretary (BNR16)
40. Sampling methodologies to select notifications to be reviewed (BNR16)
41. Copies of the notification(s) sent by the BA (or subcontractor) to the CE (or BA for breaches by subcontractors) (BNR17)
42. Use sampling methodologies to select notifications sent by the BA (or subcontractor) to the CE (or BA for breaches by subcontractors) to be reviewed (BNR17)
43. Documentation of any such law enforcement statement about delayed notification of a breach of unsecured PHI (BNR18)
44. Use sampling methodologies to select notifications to be reviewed (BNR18)
45. Documentation to prove CE or BA took correct action (BNR19)

APPENDIX B2

PRIVACY AUDIT REQUEST DOCUMENTS

1. Underwriting policies and procedures related to use and disclosure of genetic information (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials) (P1)
2. P&P regarding use and disclosure of PHI including, deceased individual's PHI, personal representative (PR) (P2) (P3)
3. Sample for compliance where PR request was recognized by the entity (P3)
4. Sample for compliance where PR request was not recognized by the entity (P3)
5. P&P regarding requests for confidential communications (P4)
6. Sample of confidential communications requests made by individuals (P4)
7. Sample of communications to individuals where a confidential communications request was accepted (P4)
8. P&P regarding PHI uses and disclosures, evaluate if constant with notice of privacy practice (NPP) (P5)
9. Documentation of disclosures by a workforce member not otherwise permitted by the privacy rule that the entity determined to meet the requirements of this standard (whistleblower) (P6)
10. P&P related to disclosure of PHI by workforce members who are a victim of a crime (P7)
11. P&P related to identification and engagement of business associates (BAs) and establishment of business associate agreements (BAAs) (P8)
12. Sample of BAA to evaluate compliance with performance criteria and P&P (P8)
13. BAA between CE and BA to include provisions for subsequent BAs/subcontractors to provide adequate assurances (P8)
14. Documentation of any material breach with BAs (P8)
15. Documentation of reports from BA to CE of uses or disclosures not provided in its contract (P8)
16. Group health plans documents for restrictions on uses and disclosure of PHI in compliance with PC (P9)
17. P&P restrict use of PHI to appropriate function being performed (e.g., provider, health plan, clearinghouse) (P10)
18. P&P related to uses and disclosures of PHI for treatment, payment, and/or operations (TPO) (P11)
19. Sample of completed consents, if any, and patient intake materials (P12)
20. P&P for obtaining a valid authorization as required by the standard, including seeking authorizations from individuals (P13) (P15)
21. Sample of a standard covered entity authorization (P13)
22. Sample of authorizations obtained (by a patient or third party) to permit disclosures (P13)
23. For providers only: All relevant patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any (P13)
24. Sample of compound authorizations (research related), if any (P14)
25. P&P related to seeking authorizations from individuals (P15)
26. Sample of conditioned authorizations (probably health plan or research related) (P15)
27. Sample of conditioned authorizations to assess exceptions (P15)

28. Sample of authorizations used as a basis for disclosure (P16)
29. Sample of the directory on a certain date along with an individual's objections (P17)
30. P&P for use and disclosures, including: address determining if individual has objected to use and disclosure for facility directory and documentation of such determination; to disclose directory in emergency, those to family members, relatives, close friends or others identified by the individual; determining or inferring individual agreement or lack objection to disclosure of PHI with individual present; disclosing only relevant info to persons when individual is not present; disclosure of PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts; documenting the individual's prior expressed preference and relationship of family members and other persons to the individual's care or payment for care; uses and disclosures for victims of abuse neglect or domestic violence pursuant to judicial or administrative proceedings and law enforcement purposes; neglect or domestic violence pursuant to judicial or administrative proceedings and law enforcement purposes; how the CE determines whether and how to make disclosure about victims of abuse, neglect or domestic violence; using or disclosing PHI for health oversight activities; disclosures during administrative or judicial proceeding; disclosures of PHI for law enforcement purposes; to disclosures of PHI to law enforcement officials for identification and location purposes; disclosing PHI to a possible victim of a crime in response to a law enforcement request; disclosures of PHI to law enforcement officials that address the requirement for an individual who has died as a result of suspected criminal conduct; disclosures of PHI about an individual who may have committed a crime on the premises to law enforcement officials; disclosures of what information about a medical emergency is necessary to disclose to alert law enforcement of PHI to law enforcement officials; disclosures of PHI to coroners and medical examiners and funeral directors; disclosures of PHI for purposes of cadaveric organ, eye, or tissue donation; disclosures for military and veterans purposes; disclosures for national security and intelligence activities and purposes; disclosure of PHI for protective services; use and disclose PHI medical suitability determinations if the CE is a component of the Department of State; correctional institution or individual in custody; disclosures of PHI for Workers' Comp or other similar programs (P17) (P18) (P19) (P20) (P21) (P22) (P23) (P24) (P25) (P26) P27) (P28) (P29) (P30) (P31) (P32) (P33) (P34) (P35) (P36) (P39) (P40) (P41)(P42)(P43) (P45)
31. Sample of public health uses and disclosures, to include uses and disclosures to an employer about an individual who is a member of the workforce of the employer (P25)
32. Sample of disclosure made for health oversight activities (P27)
33. If CE is a health oversight agency, the P&P for using PHI for health oversight activities (P27)
34. Sample of uses made for health oversight activities (P27)
35. Sample of disclosures and the corresponding court orders, subpoenas, or discovery requests (P28)
36. Sample of disclosures and the corresponding court orders, subpoenas, disclosure requests, etc (P29)
37. Sample of responses to law enforcement officials request for PHI for identification and location purposes (P30)
38. Samples of responses to law enforcement related to disclosing PHI to a possible victim of a crime in response to a law enforcement request (P31)
39. Sample of documentation of a disclosure for an individual who has died as a result of suspected criminal conduct disclosure (P32)
40. Sample documentation related to disclosures of PHI about an individual who may have committed a crime on the premises to law enforcement officials (P33)
41. Sample documentation related to disclosures of what information about a medical emergency is necessary to disclose to alert law enforcement of PHI to law enforcement officials (P34)
42. Sample documentation of disclosures of PHI to coroners and medical examiners and funeral directors (P35)

43. Sample of disclosures of PHI to organ procurement organizations (P36)
44. P&P for CE to disclose PHI for research purposes (P37)
45. Authorization, or waiver of the authorization, has been approved by an IRB or appropriately configured privacy board (P37)
46. From researchers, the required representations regarding reviews preparatory to research on decedents (P37)
47. Entity obtained the necessary authorization and/or waiver to conduct the research (P37)
48. Board approval of a waiver of authorization (P37)
49. Use or disclosure is solely to review PHI as necessary to prepare a research protocol (P37)
50. Representation that the use or disclosure is solely for research on the PHI of decedents (P37)
51. P&P to determine what documentation of approval or waiver for research purposes is needed to permit a use or disclosure and to apply that determination (P38)
52. Sample documentation of any approval or waiver for research purposes that contains all the information necessary to permit a use or disclosure (P38)
53. List of uses and disclosures for military and veterans activities (P39)
54. Sample documentation related to correctional institution or individual in custody (P43)
55. P&P related to uses and disclosures if a CE is a health plan that is a government program providing public benefits, or is it a government agency administering a government program providing public benefits (P44)
56. Sample documentation of uses and disclosures if a CE is a health plan that is a government program providing public benefits, or a government agency administering a government program providing public benefits (P44)
57. Sample documentation related to disclosures of PHI for Workers' Comp or other similar programs (P45)
58. P&P related to de-identification of PHI and re-identification of PHI (P46)
59. P&P related to limiting access to PHI (P47)
60. Sample documentation of workforce members access to PHI for their corresponding job title and description (P47)
61. P&P related to minimum necessary use or disclosure of PHI and to limit the PHI requested to the amount minimally necessary to achieve the purpose of the disclosure to minimum necessary uses and disclosures or requests for entire medical record (P48) (P49) (P50)
62. Sample of protocols for disclosures made on a routine and recurring basis and determine if they limit PHI (P48)
63. Sample of requests made on a routine and recurring basis to determine if minimum necessary followed (P41)
64. Sample documentation related to the use, disclosure, or request for an entire medical record (93)
65. P&P related to limited data sets and data use agreements if there any data use agreements in place between CE and its recipients (P51)
66. A sample data use agreement (P51)
67. A sample limited data set (P51)
68. P&P and notice of privacy practices (NPP) for disclosures of PHI to BA or institutionally related foundations (P52)
69. A sample of communications for fundraising purposes to determine if it contains a clear and conspicuous opportunity to opt out of further fundraising communications or reference to a mechanism for opting out (P52)
70. Documentation that the P&P are conveyed to the workforce (P52)

71. P&P related to a health plan addressing limitations on use and disclosure of PHI for underwriting and other purposes (P53)
72. P&P if health insurance or health benefits are not placed with the health plan limiting further use or disclosure for such purpose or as may be required by law (P53)
73. P&P in (§ 164.502(a)(5)(i)) regarding underwriting and GINA subject to the prohibition (P53)
74. P&P regarding verification of the ID of persons requesting PHI (P54)
75. Sample documentation of how the CE has verified several requestors, could include copy or notation of official credentials, a completed verification checklist, a copy of the request on official letterhead, etc. (P54)
76. Obtain a copy of NPP to validate required elements. Provide all copies of NPP (translated, etc) (P55)
77. **Question from July 2016 audit: Upload a copy of all notices posted on web site and within the facility, as well as the notice distributed to individuals, in place as of the end of the previous calendar year**
78. P&P for provisions of notice—health plans regarding the provision and posting of the NPP (P55)
79. For a sample of individuals, obtain and review documentation of when and how notices were provided (P55)
80. As part of a standard mailing sent to new health plan members, provide a NPP to the selected individuals (P55)
81. **Question from July 2016 audit: P&P in place regarding the NPP (P57) (P58) (P60)**
82. Sample acknowledgment of receipt of NPP and documenting showing a good faith effort was made when an acknowledgment could not be obtained (P57)
83. A sample population of documentation for new individuals to determine if initial date of service corresponds with date NPP was received, if they do not match was the first encounter an emergency or other explanation (P57)
84. Documentation related to provision of NPP to patients who present as an emergency (P57)
85. Observe the web site to determine if the NPP 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 NPP (P58)
86. Documentation of the agreement with the individual to receive the notice via e-mail or other electronic form; if the CE has experienced failures when trying to provide the NPP by e-mail documentation of its attempts to provide a paper copy of the notice via alternative means (e.g., mail) (P58)
87. **Question from July 2016 audit: Upload the URL for the entity web site and the URL for the posting of the entity notice (NPP), if any (P58)**
88. **Question from July 2016 audit: If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically (P58)**
89. **Question from July 2016 audit: Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form (P58)**
90. P&P for joint notice by separate covered entities. For CEs that participate in an OHCA use a joint NPPs (P59)
91. Applicable documentation criteria for NPP are established and communicated to the workforce (copies of all applicable notices and sample of acknowledgments) (P60)
92. P&P permitting an individual to request a restriction on the use of PHI for TPO; and for terminating restrictions; documenting and maintaining documentation on restriction requests (P61) (P62) (P63)
93. Sample of documentation of each request and subsequent agreement to determine if restrictions are given effect (P61)

94. All requests since September 23, 2013, for restrictions to a health plan for an item or service that has been paid out of pocket (P61)
95. Documentation to see if such restrictions were given effect (P61)
96. Sample documented terminated restriction (P62)
97. Has the CE agreed to any restrictions in the past six years? (P63)
98. P&P permit individuals to request alternative means or locations to receive communications of PHI (P64)
99. Sample requests for alternative means or locations to receive communications of PHI and the covered entity response (P64)
100. **Question from July 2016 audit: Upload all documentation related to the first five access requests that were granted, and evidence of fulfillment, in the previous calendar year. (P65)**
101. **Question from July 2016 audit: Upload all documentation related to the last five access requests for which the entity extended the time for response to the request (P65)**
102. **Question from July 2016 audit: Upload any standard template or form letter required by or used by the CE to document access requests (P65)**
103. **Question from July 2016 audit: Upload the notice of privacy practices (NPP) (P65)**
104. **Question from July 2016 audit: Upload policies and procedures for individuals to request and access to protected health information (PHI) (P65)**
105. P&P for individuals to request and obtain access to PHI and denial of access ensuring timely, written denials with all required elements; dictating when denials of requests for access are unreviewable; reviewable grounds for denial of access; request for and fulfillment of instances of denial of access; if a person or office is specified to process requests for access (P65)(P66) (P67) (P68) (P69)(P70)
106. NPP for correct reference to access rights (P65)
107. Access requests that were granted and documentation of fulfillment if any, and access requests that were denied to determine whether response was made in a timely manner. (e.g., within 30 days of request receipt, unless extension provided (P65)
108. A standard form for individuals requesting access to their PHI (P65)
109. Sample of denied access requests (P66)
110. Documentation of the current designated record sets subject to access requests along with documentation for last six years (P70)
111. Name or office for each of the last six years that process access requests (P70)
112. P&P allowing an individual the right to amend protected health information in a designated health record set and circumstances which the entity has grounds for denial of amendment; denial of amendment request (P71) (P72) (P74)
113. Sample of requests by individuals to amend their PHI in a designated record set (P73)
114. Sample of requests related to denials of amendments (P74)
115. P&P in place to document and respond to an accounting of disclosures (AOD) request, including limiting grounds for denial; to provide individual with timeliness and fees for AOD (P75)(P76) (P77)
116. Sample of request for AOD and the entity fulfillment of those requests (P76)
117. Documentation of who is responsible for development and implementation of P&P (P79)
118. Documentation of what person or office is designated to receive complaints; how complaints are received, processed, and documented (P79) (P82)

119. Documentation of development and implementation of P&P and complaints are maintained in electronic or written form for six years (P79)

120. P&P related to training its workforce as necessary and timely (P80)

121. From the population of new hires within specified audit period a sample of the documentation of training on the HIPAA privacy rule that was provided and completed (P80)

122. Documentation that workforce members have been trained on material changes to P&P (P80)

123. P&P to determine if appropriate administrative, technical, and physical safeguards are in place (P81)

124. Documentation of specific safeguards from all three categories to reasonably protect PHI. Such documentation may include, but is not limited to P&P, photographic, or documentary documentation of physical and technical safeguards and statements from privacy and security officials (P81)

125. Sample of documentation of complaints (P83)

126. P&P to determine if the entity has applied sanctions (P84)

127. Documentation of applicable sanctions to a sample of workforce members to determine if appropriate sanctions were applied (P84)

128. Documentation related to a CE mitigating any harmful effect known to the CE of a use or disclosure by CE or BA in violation of P&P (P85)

129. Documentation that a process is in place to ensure mitigation actions are taken pursuant to the P&P (P85)

130. From a population of noncompliance within the audit period whether mitigation plans were developed and applied pursuant to the P&P (P85)

131. Documentation that P&P are conveyed to workforce (P85)

132. P&P in place in relation to anti-intimidation and anti-retaliatory standards (P86)

133. Documentation that P&P related to anti-intimidation and anti-retaliatory standards are conveyed to the workforce (P86)

134. P&P and patient health plan/member info to ensure that a waiver of their right to complain is not required as a condition of treatment, payment, or enrollment in a health plan or eligibility for benefits (P87)

135. P&P with respect to PHI designed to comply with the requirements of the HIPAA privacy rule including evidence that P&P are reasonably designed to ensure compliance for size and types of activities performed, that the entity changes promptly these P&P as necessary to comply with changes in the law, that any corresponding changes are made to the NPP as applicable (170)

136. Copies of P&P from the previous calendar year and January 1, 2012 and the corresponding NPP in effect for those dates illustrating that material changes, e.g., for health plans limits on genetic info for underwriting, for providers that a request for restriction must be accepted in certain situations are incorporated into the P&P (P88)

137. Documentation of maintenance all required P&P written communications and documentation in written or electronic form (P89)

APPENDIX B3

SECURITY AUDIT REQUEST DOCUMENTS

1. **Question from July 2016 audit: P&P regarding the entity's risk analysis process (S2)**
2. **Question from July 2016 audit: Documentation demonstrating that P&P related to security risk analysis were in place and in force six years prior to the date of receipt of notification (S2)**
3. **Question from July 2016 audit: Documentation of risk analysis results from the previous calendar year and that such documentation is available to the persons responsible for this implementation and that such documentation is periodically reviewed and, if needed, updated (S2)**
4. **Question from July 2016 audit: Upload documentation of the current risk analysis and the most recently conducted prior risk analysis (S2)**
5. **Question from July 2016 audit: Upload documentation of current risk analysis results (S2)**
6. Obtain risk analysis P&P; upload policies and procedures regarding the entity's risk analysis process (S2)(S4)
7. P&P related to security variations and evaluation of compliance with PC for countermeasures or safeguards implemented. **Question from July 2016 audit: Documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment (S3)**
8. **Question from July 2016 audit: Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment (S3)(S5)**
9. Documentation demonstrating these P&P have been implemented and that the processes match the P&P (S3)
10. **Question from July 2016 audit: Documentation demonstrating that policies and procedures related to reducing risk as result of a security risk analysis and mitigation/remediation of its results are in place and in force six years prior to the date of receipt of notification (S3)**
11. **Question from July 2016 audit: Documentation demonstrating the efforts used to manage risk during the previous calendar year (S3)**
12. **Question from July 2016 audit: P&P related to the risk management process (S3)(S5)**
13. **Question from July 2016 audit: Documentation demonstrating that current and ongoing risks reviewed and updated (S3)**
14. **Question from July 2016 audit: Documentation from the previous calendar year demonstrating that documentation related to reducing risk as result of a security risk analysis and mitigation/remediation of its results is available to the persons responsible for security risk analysis and the risk reduction processes and that such documentation is periodically reviewed and, if needed, updated (S3)**
15. P&P addressing purpose and scope, workforce member responsibility, management involvement and how frequently the analysis is reviewed and updated (S4)
16. Written risk analysis documents or other records that document an accurate assessment was conducted that contains: a. Defined scope of all systems that create, transmit, maintain or transmit ePHI b. Details of identified threats c. Assessment of current security measures d. Impact and likelihood analysis e. Risk rating (S4)
17. If there is no prior risk analysis or other record, obtain and review the two most recent written updates to the risk analysis or other record, if any (S4)
18. 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 (S4)
19. Sanctions P&P (S6)

20. Documentation demonstrating sanctions applied to workforce members (S6)
21. P&P related to records of info systems activities (S7)
22. Documentation of reviews of info system activity such as audit logs, access reports, security incident tracking (S7)
23. Documentation demonstrating capabilities of the info system logs (S7)
24. Documentation of the security official's responsibilities (e.g., job description) (S8)
25. P&P ensuring all workforce members have access to ePHI required to perform their job (S9)
26. Documentation of access granted to workforce members and correlation to their job duties (S9)
27. Documentation demonstrating management reviews access levels for systems with ePHI that access is appropriate (S9)
28. P&P related to authorization/supervision of workforce members (S10)
29. Documentation of how requests for access to ePHI are processed (S10)
30. Identification of who has the authorization and/or supervisory permission to approve. Access to information systems and/or locations where ePHI may be accessed (S10)
31. Documentation demonstrating how access requests to locations where ePHI might be accessed are processed (S10)
32. Documentation of workforce members who were authorized to access ePHI or locations where ePHI might be accessed and organizational charts/lines of authority (S10)
33. If an alternative measure (addressable) has been implemented, produce documentation of why the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented (S10) (S11)(S12)(S15)(S16)(S18)(S19)(S20)(S21)(S28)(S29)(S34)(S35)(S36)(S37)(S43)(S44)(S48)(S49)(S52)(S55)(S56)
34. Documentation related to workforce clearance procedures and whether they work to determine whether access is appropriate (S11)
35. Documentation demonstrating use of workforce clearance in granting appropriate access to ePHI (S11)
36. Documentation demonstrating approval or verification of access to ePHI (e.g., approved access request forms, electronic approval workflow, etc.) (S11)
37. Documentation that access was terminated (S12)
38. Documentation demonstrating changes in access levels for workforce members with ePHI access (S12)
39. Documentation of the job duties of workforce members before and after ePHI access level was changed (S12)
40. P&P to determine that access is reasonably and appropriately restricted to those that need access (S13)
41. P&P for minimum necessary (S13)
42. Access controls that support minimum necessary (S13)
43. P&P related to protecting ePHI held by clearinghouse from unauthorized access by the larger organization (S14)
44. P&P regarding workforce member access to ePHI (S15)
45. Procedures to create, enable, modify, disable, and remove information system accounts (S15)

46. Documentation associated with granting access to ePHI (S15)
47. P&P and evaluate content relative to PC for authorizing access, documenting, reviewing, and modifying user access to workstation, transaction, program, or process (S16)
48. Documentation regarding individuals whose access to info systems has been reviewed based on access authorization P&P (S16)
49. Documentation of individuals whose access has been modified based on access P&P (S16)
50. P&P for security awareness and training program (S17)
51. Documentation demonstrating implementation of security and awareness program including related training materials (S17)
52. Documentation demonstrating that security awareness programs are provided to the entire organization and BA if appropriate (S17)
53. Documentation of how periodic security reminders are conducted (S18)
54. Documentation demonstrating that periodic security updates are conducted (S18)
55. Procedures against detecting and reporting malicious software are incorporated into security training (S19)
56. Documentation of the workforce members who should be trained on procedures to guard against, detect, and report malicious software (S19)
57. Procedures (or other vehicle) for monitoring login and reporting discrepancies and related training materials (S20)
58. Documentation demonstrating procedures in place to monitor login attempts and report discrepancies (S20)
59. Documentation of workforce members' role types and who should be trained about monitoring and reporting login attempts (S20)
60. Password management procedures and training for creating, changing, and safeguarding passwords (S21)
61. Documentation demonstrating procedures for creating, changing, and safeguarding passwords are in place (S21)
62. Documentation of workforce members and role types who should be trained on password management (S21)
63. Documentation of the workforce members who were trained on password management (S21)
64. P&P related to security incidents (S22)
65. Documentation demonstrating security incident P&P are implemented (S22)
66. Documentation of responding to, reporting, and mitigating security incidents (S23)
67. P&P related to formal contingency plan (S24)
68. Documentation demonstrating that a contingency plan is implemented (S24)
69. P&P related to data back-up plans (S25)
70. Documentation demonstrating how data is backed up (S25)
71. Documentation demonstrating data backup and restoration tests (S25)

72. Documentation related to a disaster recovery plan (S26)
73. Procedures for restoring lost data (S26)
74. Documentation of data restore tests and test results (S26)
75. Procedures related to an emergency mode operation plan (S27)
76. Documentation demonstrating business continuity while in emergency mode (S27)
77. P&P related to periodic testing and revision of contingency plans (S28)
78. Documentation demonstrating the revision of contingency plans (S28)
79. Documentation of contingency plan tests and related results (S28)
80. Documentation of critical ePHI applications and their assigned criticality levels (S29)
81. Documentation of the procedures regarding how ePHI applications (data applications that store, maintain, or transmit ePHI) are identified (S29)
82. Documentation of P&P related to technical and nontechnical evaluation (S30)
83. Documentation demonstrating periodic technical and nontechnical evaluations (S30)
84. Documentation of procedures for technology change control/management and documentation of major technology changes which affected the security of ePHI (S30)
85. Documentation of plans related to risk management or mitigation efforts in response to evaluations conducted due to a major technology change which affected the security of ePHI (S30)
86. Documentation identifying all business associates (S30)
87. BAA and/or contracts (S30)
88. This inquiry is for BAs only: determine whether the BA contract identifies if it utilizes any subcontractors and review the BAA (S30)
89. Documentation of all BAs (S32)
90. Written agreements or other arrangements (i.e., a MOU if the CE and BA are government agencies) (S32)
91. This inquiry is for BAs only: written contract or other arrangement identifies if there are any subs, if so review the written contract or other arrangement (S32)
92. P&P regarding facility access control (S33)
93. Documentation of workforce members with authorized physical access to electronic information systems and the facility or facilities in which they are housed (S33)
94. Documentation of procedures for granting individuals access to entity facility or facilities where electronic information systems are housed (S33)
95. Documentation of visitor physical access to electronic information systems and the facility or facilities where it is housed (S33)
96. Contingency operations procedures (S34)
97. Documentation demonstrating contingency operation procedures currently implemented (S34)
98. Documentation demonstrating that contingency operation procedures are tested (S34)
99. P&P related to the facility security plan (S35)

100. Documentation demonstrating that facility security plan procedures are implemented to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft (S35)
101. Procedures related to access control and validation documentation demonstrating the control of visitors' physical access to facilities (S36)
102. Documentation demonstrating control of access to software program for modification and revision (S36)
103. Documentation demonstrating facility and software access control and validation procedures are implemented (S36)
104. P&P related to maintaining maintenance records (S37)
105. Documentation demonstrating records of repairs and mods to physical security components (S37)
106. P&P related to workstation use (S38)
107. Procedures related to the proper use and performance of workstations (S38)
108. Inventory of the locations and types of workstations (S38)
109. Documentation demonstrating workstation classification (S38)
110. Documentation demonstrating workstation use policies and procedures implemented (S38)
111. P&P related to workstation security (S39)
112. Documentation demonstrating workstation security P&P being implemented (S39)
113. P&P related to device and media controls (S40)
114. Documentation demonstrating the movement of hardware and electronic media containing ePHI into, out of, and within the facility (S40)
115. Documentation demonstrating the type of security controls implemented for the facility in, out, and within movements of workforce members' assigned hardware and electronic media that contain ePHI (S40)
116. P&P related to disposal of any electronic media that stores ePHI (S41)
117. Documentation demonstrating how the disposal of hardware, software, and ePHI data is completed, managed, and documented (S41)
118. Documentation demonstrating how the sanitization of electronic media is completed, managed, and documented (S41)
119. Procedures related to media re-usage (S42)
120. Documentation demonstrating media re-use procedures being implemented and how ePHI has been removed from electronic media (S42)
121. P&P related to device and media accountability (S43)
122. Documentation demonstrating a record of movements of hardware and electronic media and person responsible therefore (S43)
123. P&P related to data backup and storage procedures (S44)
124. Documentation demonstrating how ePHI data is backed up for equipment being moved to another location (S44)
125. Documentation demonstrating how ePHI data backups for moved equipment are stored (S44)
126. Documentation demonstrating the restoration of ePHI data backups for moved equipment (S44)

127. P&P related to access control (S45)
128. Demonstrating the implementation of access controls for electronic information systems that maintain ePHI (S45)
129. Documentation demonstrating a list of new workforce members from the electronic information system who was granted access to ePHI (S45)
130. Documentation demonstrating the access levels granted to new workforce members (S45)
131. Documentation of a list of users with privileged access (S45)
132. List of default, generic/shared, and service accounts from the electronic information systems with access to ePHI (S45)
133. Documentation demonstrating the access levels granted to default, generic/shared, and service accounts (S45)
134. Documentation demonstrating that periodic reviews of procedures related to access controls have been conducted (S45)
135. Documentation demonstrating a list of terminations and job transfers (S45)
136. Documentation demonstrating the removal or modification of user access levels (S45)
137. P&P regarding the assignment of unique user IDs (S46)
138. Documentation demonstrating the assignment, creation, and use of unique user IDs (S46)
139. Procedures in place to provide necessary access to ePHI during an emergency (S47)
140. Documentation demonstrating a list of workforce members with authority to initiate the emergency access procedures (S47)
141. Documentation demonstrating technical systems limiting emergency access initiation (S47)
142. P&P regarding automatic logoff (S48)
143. Documentation (e.g., screenshots, system settings, etc.) demonstrating the implementation of automatic logoff (S48)
144. P&P regarding the encryption and decryption of ePHI (S49)
145. Documentation demonstrating ePHI being encrypted and decrypted (S49)
146. Documentation relative to audit controls (S50)
147. Documentation demonstrating the implementation of hardware, software, and/or procedural mechanisms to record and examine activity (S50)
148. P&Ps regarding the implementation of integrity controls to protect ePHI (S51)
149. Documentation demonstrating processes in place to protect ePHI from improper alteration or destruction (S51)
150. P&P for authenticating ePHI (electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner) (S52)
151. Documentation demonstrating that electronic mechanisms are implemented to authenticate ePHI (mechanisms to determine that appropriately corroborate that ePHI has not been altered or destroyed in an unauthorized manner) (S52)
152. P&P regarding person or entity authentication (able to verify that a person or entity seeking access to ePHI is the one claimed) (S53)

153. Documentation demonstrating the implementation of authentication procedures for persons or entities seeking access to ePHI (S53)
154. P&P related to transmission security controls (S54)
155. Identify the various methods, devices, and networks used to electronically transmit ePHI (S54)
156. Identify the technical security controls implemented to guard against unauthorized access to ePHI transmitted over electronic communication networks (S54)
157. Documentation demonstrating the implementation of technical security measures to protect electronic transmissions of ePHI (S54)
158. P&P related to transmission security measures (S55)
159. Documentation demonstrating the implementation of security measures to protect electronic transmissions of ePHI (S55)
160. P&P regarding the encryption of electronically transmitted ePHI (does the entity have encryption mechanism to encrypt ePHI whenever deemed?) (S56)
161. Documentation demonstrating the encrypted mechanism is implemented to encrypt ePHI (S56)
162. Documentation demonstrating that electronically transmitted ePHI is encrypted (S56)
163. P&P in place regarding its contractual arrangements with contractors or other entities to which it discloses ePHI for use on its behalf (S57)
164. The entity's standard business associate contract template(s) (S57)
165. Documentation demonstrating the entity's approval process when deviations affecting the implementation of safeguards (by the BA?) to protect ePHI are considered (S57)
166. Obtain BA contracts (S58)(S59)(S60)
167. Documentation demonstrating that the entity's business associates have reported security incidents of which it was aware, including breaches of unsecured PHI (S60)
168. P&P in place regarding other arrangements to have in place (e.g., a MOU if the CE and BA are government agencies) (S61)
169. Documentation of the entity's other arrangements with BAs (S61)
170. BA contracts entered into with subcontractors (S62)
171. P&P in place to ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan (S63)
172. Review plan documents (S63)
173. Review plan documentation (language that requires the sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan) (S64)
174. Health plan documentation (ensure adequate separation between the group health plan and the plan sponsor) (S65)
175. Health plan documentation (incorporate provisions that requires the sponsors to ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures) (S66)

176. Health plan documentation (language that requires plan sponsors to report to the group health plan any security incident of which it becomes aware) (S67)
177. Documentation of the policies and procedures regarding the implementation of compliant P&P (S68)
178. P&P regarding the maintenance of P&P (S69)
179. Documentation demonstrating that P&P are being maintained (S69)
180. Written documentation demonstrating the entity's action, activity, or assessment that is required by the security rule (S69)
181. Documentation of P&P for compliance with retention requirements (S70)
182. Documentation demonstrating that P&P are being maintained for six years from the date of its creation or the date when it last was in effect (S70)
183. Documentation demonstrating that an action, activity, or assessment is being maintained for six years from the date of its creation or the date when it last was in effect (S70)
184. Documentation of P&P regarding the availability of documentation (S71)
185. Documentation demonstrating that security rule P&P are made available to the workforce members responsible for implementing the pertaining procedures (S71)
186. P&P regarding documentation reviews and updates to security P&P (S72)
187. Documents demonstrating that P&P are reviewed and updated on a periodic basis (S72)

APPENDIX C

PRIVACY AND SECURITY COMPLIANCE PROGRAM MASTER POLICY TEMPLATE

Coverage

(Insert Name) (hereafter referred to as the 'organization') workforce members that access, use or disclose confidential patient information.

Reviewed/Revised

(Insert Date)

Purpose

This policy establishes a privacy and security compliance program (plan), including reporting and accountability structure in order to facilitate compliance with the appropriate security regulations mandated by both federal (typically HIPAA) and state regulators.

Policy

In this organization, the security officer's role is directly related to data and hardware, mobile devices, network, software, back-ups, and device security while the privacy officer is responsible for providing direction and oversight of the processes that impact confidentiality and related safeguards of patient data, as well as, rights afforded under HIPAA. Privacy and security officers work together to create a program of compliance that facilitates meeting all regulatory mandates.

The security officer activities will include implementing, monitoring, and maintaining compliance with this organization's security compliance program policies and procedures. Privacy compliance program duties, such as, breach determination, notification along with investigation, mitigation and sanction related duties are performed by the privacy officer. In smaller organizations the privacy and security officer can be the same person. These officers will be established at the direction of the CEO/board of directors or their designee and have clear reporting and governance with these parties.

The HIPAA privacy and security officers' duties include:

- Manage all HIPAA related compliance activities.
- Implement and manage all HIPAA privacy and security rule related administrative, technical, and physical safeguards, as they apply to this organization for both PHI (protected health information) and ePHI (electronic protected health information).
- Development, implementation, and maintenance of appropriate privacy and security related policies and procedures.
- Conduct various risk analysis, as needed or required.
- Manage HIPAA violation and breach notification investigations, determinations, and responses, including breach notifications.
- Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.
- Ensure consistent application of sanctions for failure to comply with privacy policies for all individuals in this organization's workforce, in cooperation with human resources, the information security officer, administration, and legal.
- Administer patient requests related to patient rights under HIPAA privacy.
- Administer the process for receiving, documenting, tracking, investigating, and taking action on all privacy complaints in conjunction with HR, other compliance officers, and legal counsel.
- Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.

- Develop additional relevant policies, such as policies governing the inclusion of confidential data in e-mails, and access to confidential data by telecommuters.
- Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- Conduct periodic privacy audits and take remedial action as necessary.
- Remediate and mitigate discovered privacy and security violations according to organizational policy.
- Provide for uniform enforcement of sanctions brought on by privacy or security violations.
- Oversee employee training in the areas of information privacy and security.
- Deter retaliation against individuals (patients) who seek to enforce their own privacy rights or those of others.
- Remain current and advise on new technologies to protect data privacy.
- Remain current in reference to laws, rules and regulations regarding security and privacy, updating this organization's policies and procedures as necessary.
- Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns.
- Ensure business associates (or if a BA) sub-contractors have necessary privacy and security compliance programs. Ensure business associate agreements (or sub-contractors agreements if a BA) are in place, monitored, and enforced.
- Ensure group health plans and MOUs with government entities are compliant with HIPAA and afford the highest levels of protections.

This organization willfully document all HIPAA compliance related activities and efforts, in accordance with appropriate policies. All HIPAA compliance related investigation documentation will be retained for at least the timeframe required by regulation from the date of creation or last revision, whichever is later and in accordance with the organization's document retention policy.

The security compliance program is governed by a structure that fosters organization wide workforce participation to support ongoing compliance with regulatory requirements.

1. Security and privacy compliance program governance and staffing shall be defined and appointed by the CEO/Board of Directors or their designee.

   Organizational stakeholders involved in privacy and security compliance program governance shall represent be represented by management staff including, but not limited to:

   i. Administration
   ii. Security officer
   iii. Privacy officer
   iv. Senior corporate compliance officer
   v. Health information management
   vi. Risk management
   vii. Medical staff services
   viii. Information systems
   ix. Nursing
   x. Human resources

2. Organizational governance of the privacy and security compliance program (plan) shall undertake, but not be limited to:
   a. Meeting on a regular basis and as needed for urgent events.
   b. Meetings have established procedures for recording of meeting minutes.
   c. Provide guidelines for implementation of security (and related privacy) compliance policies and procedures in accordance with federal and state laws, regulations, and accreditation standards.
   d. Communication and propagation of privacy and security compliance policies and procedures.
   e. Establish procedures, guidelines, tools, reports, to monitor compliance with privacy and security compliance program policies and procedures.
   f. Review violation issues/trends concerning security and related privacy compliance within the organization with recommendation and follow-up of corrective action with appropriate personnel. Document and appropriately report all findings.
   g. Privacy and security incidents will be managed by a dedicated team with dedicated tools and processes.
   h. Post security or privacy event (incident) analysis with corrective actions, mitigation, or remediation will be adopted into ongoing policies, procedures, and training.
   i. Conduct investigations in relation to breach determination, probability of compromise analysis, and breach notification as needed.
   j. Report privacy and security violations or breaches to the organization's senior corporate compliance officer, OCR, and individuals, as appropriate.
   k. Assist in OCR investigations as appropriate.
   l. Determine user group access levels necessary to carry out job responsibilities, including determination of access to confidential patients.
   m. Determine content of materials and tracking of privacy and security workforce training.
3. This organization's privacy and security compliance program will be compliant with all mandatory federal and state privacy and related security regulations, including but not limited to HIPAA. The organization recognizes its status as a covered entity <or insert business associate if appropriate> under the definitions contained in the HIPAA regulations and that they must comply with HIPAA privacy and security regulations concerning state law preemptions of HIPAA regulations. HIPAA generally preempts state laws regarding privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better access to data than HIPAA, will preempt HIPAA regulations. In general both HIPAA law and state law shall be complied with whenever possible. If there is a conflict between the two, a preemption analysis and determination, possibly involving legal counsel, must be made to assess which laws (HIPAA, state laws, or both) must be followed.
4. The privacy officer is responsible for analysis of HIPAA preemption issues, if necessary in consultation with security officer and legal counsel to make preemption determinations. The privacy officer will then create, modify, or amend organization policies and procedures to accurately reflect preemption determinations The privacy officer performs ongoing research to monitor legislative changes in the state(s) where this organization operates that may impact HIPAA preemption issues.
5. Failure for workforce members to comply with all organizational privacy and security policies and procedures will be dealt with according to defined mitigation, remediation, corrective action and sanction policy and procedures.
6. HIPAA regulations and best practices call for the creation and implementation of specific policies and procedures addressing your HIPAA privacy and security compliance and they must be followed by all workforce members. Privacy and security policies and procedures shall be updated and amended by the respective Privacy and security compliance officers and staff, as needed or as required by law. All policies and procedures shall be made accessible to appropriate members of the workforce. The organization's security compliance program will be compliant with all mandatory federal and state privacy and related

security regulations, including but not limited to HIPAA. The security compliance program follows numerous guidelines, including HIPAA security and HITECH privacy but also may include PCI and other standards for security compliance.

7. Privacy and security risk analysis will be undertaken on a routine basis in order to prioritize risks, determine mitigation priorities and reduce risks to an acceptable level. These prioritized risks will become a part of a global risk management plan. Within a security risk analysis the security rule has two types of implementation specifications, "required" and "addressable." The required specifications must be implemented. The addressable implementation specifications are not required but must be "addressed." Not being required does not mean optional; this organization has one of three courses of actions to take for addressable items, one of which must be taken. The organization will decide to implement a specification, implement an alternate equivalent, or not implement it at all. If the decision is made to implement an alternative or to not implement it at all, it is required to document the reasoning and support why an alternative method or not to implement it at all was chosen. This documentation should be kept, as with all HIPAA documentation, for six years from its creation or last revision date, whichever is later. These assessments will need to include whether technologies for security are adequate and include vulnerability scans, penetration, data network tests.
8. Covered entities (CEs) will assess and monitor business associate compliance programs (or insert BA-subcontractor if appropriate). CEs and BAs will agree upon breach discovery timeframes, breach determination processes and which party is to provide notifications. Note: Under HIPAA omnibus final rules CEs, BAs, and subcontractors are all directly liable for their HIPAA compliance.
9. HIPAA rules are flexible in relation to the actual implementation of required rules; larger organizations will need to utilize more sophisticated methodologies. Although it must be recognized that all rules are required to be met at all times what is considered "reasonable" and appropriate may vary by organization type, size and nature of the PHI they manage.
10. Any healthcare clearinghouses owned or affiliated with this organization will have separate staff, physical space, ePHI, and compliance plans.
11. Workforce HIPAA training
12. Security standards to be maintained per HIPAA security rules (§164.306) in reference to the organization's security compliance program:
    a. General requirements. Covered entities must do the following:
        (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the CE creates, receives, maintains, or transmits.
        (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
        (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
        (4) Ensure compliance with this subpart by its workforce.
    b. Flexibility of approach.
        (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
        (2) In deciding which security measures to use, a CE must take into account the following factors:
            (i) The size, complexity, and capabilities of the CE.
            (ii) The CE's technical infrastructure, hardware, and software security capabilities.
            (iii) The costs of security measures.
            (iv) The probability and criticality of potential risks to electronic protected health information.

E. Related Procedures

- *Insert any general HIPAA compliance procedures utilized to facilitate privacy and security compliance.*
- *Insert workforce training program details (who is trained, on what subjects, how often).*
- *< Sample language below; determine if to be used by each site, if so change to black font and adopt as a procedure>*
  - *Privacy/security event (or incident) management procedure*
    - *Detect a potential security violation or receive a security or privacy event reporting form from the workforce or other complainant.*
    - *Document the investigation of this compliant using the security or privacy event management form*
    - *Perform corrective actions, mitigations, and sanctions as needed to respond to this event (incident).*
    - *Report as contractually obliged under the business associate agreement to the client/covered entity if potentially a privacy violation or breach of PHI (protected health information).*
    - *Retain the documentation of the compliant (or report) for mandatory HIPAA retention period (six years).*

F. Related Forms

- ROI, breach, and patient's rights log
- Security or privacy reporting
- Investigation and corrective actions of security/privacy event
- Request for patient's rights
- Breach determination and reporting form

Related Policies

- Documentation for privacy compliance
- HHS, OCR, or other regulatory investigations
- Breach determination and reporting
- Sanctions, enforcement, and discipline
- HIPAA privacy awareness workforce training
- Security incident reporting
- Security officer job description
- Combined privacy and security job description for physician practice

References

- CompliancePro Solutions™ Security Risk Analysis™ (SRA) tool
- 45 CFR 164.302–164.318
- 45 CFR Parts 160 and 164 (HIPAA) §164.530§ 164.104, § 164.306, § 160.201 to § 160.205
- HITECH Act § 13401,
- HIPAA laws fostering Policies and Procedures § 160.310, § 164.306, § 164.312, § 164.316 and § 164.530(i)
- 45 CFR Parts 160 and 164 (HIPAA) §164.530
- §164.306–Security standards: General rules
- NIST Incident Handling SP800-61 Rev 2
- 2013 Omnibus HIPAA Privacy Final Rules

APPENDIX D

SAMPLE (CHIEF) PRIVACY OFFICER JOB DESCRIPTION

Position Title: (Chief) Privacy Officer*

Immediate Supervisor: Chief executive officer, (chief) compliance officer, senior executive (chief operating officer, CIO), (senior) in-house counsel, or practice manager

Position Overview: Under HIPAA (the Health Insurance Portability and Accountability Act of 1996) every healthcare organization must designate a privacy official. The privacy official may have other titles and duties in addition to his/her privacy official designation in a typical practice or organizational setting. In terms of HIPAA compliance, the privacy official shall oversee all ongoing activities related to the development, implementation and maintenance of the practice/organization's privacy policies in accordance with applicable federal and state laws. HIPAA for purposes of this document includes HIPAA, HITECH, and Omnibus requirements.

General Purpose: The Privacy officer is responsible for the organization's privacy program including but not limited to daily operations of the program, development, implementation, and maintenance of policies and procedures, monitoring program compliance, investigation and tracking of incidents and breaches and insuring patients' rights in compliance with federal and state laws.

Responsibilities:

- Builds a strategic and comprehensive privacy program that defines, develops, maintains, and implements policies and processes that enable consistent, effective privacy practices which minimize risk and ensure the confidentiality of protected health information (PHI), paper and/or electronic, across all media types. Ensures privacy forms, policies, standards, and procedures are up to date.
- Works with organization senior management, security, and corporate compliance officer to establish governance for the privacy program.
- Serves in a leadership role for privacy compliance.
- Collaborates with the information security officer to ensure alignment between security and privacy compliance programs including policies, practices, investigations, and acts as a liaison to the information systems department.
- Establishes, with the information security officer, an ongoing process to track, investigate, and report inappropriate access and disclosure of protected health information. Monitor patterns of inappropriate access and/or disclosure of protected health information.
- Performs or oversees initial and periodic information privacy risk assessment/analysis, mitigation and remediation.
- Conducts related ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions.
- Takes a lead role, to ensure the organization has and maintains appropriate privacy and confidentiality consents, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
- Oversees, develops, and delivers initial and ongoing privacy training to the workforce.
- Participates in the development, implementation, and ongoing compliance monitoring of all business associates and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Works cooperatively with the health information management (HIM) director and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.

- Manages all required breach determination and notification processes under HIPAA and applicable state breach rules and requirements.
- Establishes and administers a process for investigating and acting on privacy and security complaints.
- Performs required breach risk assessment, documentation, and mitigation. Works with Human Resources to ensure consistent application of sanctions for privacy violations.
- Initiates, facilitates, and promotes activities to foster information privacy awareness within the organization and related entities.
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards.
- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.
- Cooperates with the US Department of Health and Human Services' Office for Civil Rights, State regulators and/or other legal entities in any compliance reviews or investigations.
- Serves as information privacy resource to the organization regarding release of information and to all departments for all privacy related issues.

Qualifications:

- Degree in health information management or a related healthcare field.
- Knowledge and experience in state and federal information privacy laws, including but not limited to HIPAA.
- Demonstrated organization, facilitation, written and oral communication, and presentation skills.
- Recommended privacy certification such as Certified in Healthcare Privacy and Security (CHPS) and/or other healthcare industry related credential, e.g. RHIA, RHIT.

Additional Requirements:

- Demonstrated skills in collaboration, teamwork, and problem solving to achieve goals
- Demonstrated skills in verbal communication and listening
- Demonstrated skills in providing excellent service to customers
- Excellent writing skills
- A high level of integrity and trust
- Extensive familiarity with healthcare relevant legislation and standards for the protection of health information and patient privacy
- Healthcare legal, operational, and or financial skills

This document is published in the AHIMA Body of Knowledge at bok.ahima.org/doc?oid=107672.

Notes

* The title for this position will vary from organization to organization, and may not be the primary title of the individual serving in the position. "Chief" would most likely refer to very large integrated delivery systems. The term "privacy officer" is specifically mention in the HIPAA Privacy Regulation.

APPENDIX E

HIPAA POLICY AND PROCEDURES CHECKLIST

Privacy

HIPAA privacy rights and operations guide
Security risk gap assessment policy
Documentation for security and privacy compliance
Appropriate access to PHI by workforce
Confidentiality of PHI
Minimum necessary
Designated record set
Individual (patient) access to PHI
Disclosure of PHI
Fax policy
Request for amendment of PHI
Request to restrict use and disclosure of PHI
Accounting of disclosures
Use and disclosure for marketing and fundraising
Audit controls, access and privacy monitoring
Security compliance program (plan)
Security and privacy compliance program (plan)
Complaints, privacy internal and external
Breach determination and reporting policy
Breach decision tree for omnibus breach determination
Mitigation of improper use or disclosure
Sanctions, enforcement and discipline
Investigations by HHS–OCR–Other
BAA Sample Language–CE Perspective
BAA Sample Language–BA Perspective
BAA Sample Language–BA to Subcontractor Perspective
NPP–notice of privacy practice full template
NPP summary tri-fold
NPP OCR Model 3 templates
Digital copier and device privacy
Training workforce HIPAA
E-mail policy
Business associate master policy
Photo, video, non-text management
Risk management plan

Security

Authorization to access PHI
Workforce security clearance
Workforce termination
Physical security policy
Malware protection
Log-in monitoring
Password and log-on management
Security incident management
Business continuity, data criticality, back-up, disaster recovery
Emergency access
Hardware and device management
Automatic logoff
Workstation security and use
Authentication and unique ID
Access controls
Emergency plan testing and update
Integrity controls including encryption
Maintenance records related to security
HIPAA security awareness training test (auto version)
Record retention
Security officer job description
Combined privacy and security officer job description for physicians practice
BA privacy and security compliance questionnaire
ROI, breach, and patients' rights log

APPENDIX F

HIPAA FORMS CHECKLIST

- Security and privacy certification acknowledgment
- Security or privacy reporting form
- Investigation and corrective action of security/privacy event form
- Patient right of access request form
- Denial reviewable of access request form
- Denial unreviewable of access request form
- BYOD (bring your own device) user agreement
- Request for patient's rights form
- Addendum to request for restrictions for disclosures to health plans
- Denial of amendment or restriction request form
- Authorization to disclose PHI form
- Patient request for access to PHI form
- Breach notification letter
- Breach determination and reporting form
- Denial of amendment form
- Acceptance of amendment form
- HIPAA privacy and security training presentation
- HIPAA privacy and security workforce training (auto test)
- Omnibus final rule breach assessment form (manual)
- Interim final rule breach assessment form (manual)
- Confidentiality agreement for visitors and non-workforce members
- Privacy and security rounds/physical inspection checklist
- Patient consent addendum for additional parties
- Confidentiality and security agreement
- AHIMA CEU for training form
- OCR audit protocols
- Certificate of training
- Confidentiality and security exit agreement
- Disclosures to law enforcement
- Accounting of disclosure request form

Note: This is not an all-inclusive list. Other forms may or may not be required based on organization.

APPENDIX G

SAMPLE AUDIT CONTROLS, ACCESS AND PRIVACY MONITORING PLAN

A. Coverage:

<Insert site name> (hereafter referred to as the "Organization") workforce members that use protected health information (PHI) may be subject to or assist in the performance of ongoing privacy and security audits and monitors.

B. Reviewed/Revised:

July 21, 2013

C. Purpose:

To define the policy for ongoing audit controls, as well as privacy and security auditing and monitoring to detect violations of appropriate access, use and disclosure of PHI.

D. Policy:

An ongoing audit, monitoring and evaluation process is critical in detecting noncompliance and improving the quality of work, and will help ensure the success of the Organization's privacy program. Audit controls will be utilized in various ways to ensure compliance with regulations and this organization's policies and procedures. In furtherance of its obligations as a covered entity (CE) or business associate (BA) that manages PHI, this organization will perform internal audits and ongoing monitoring to measure compliance and provide feedback in areas that are found to need continued work. This ongoing audit, monitoring and evaluation process will include the following:

1. Regular audits of compliance with the organization's privacy policies and procedures, to be conducted or directed by the privacy and security officer(s) and appropriate oversight committees
2. Special audits focusing on access to electronic records that contain PHI
3. Audits of BAs and their privacy practices, policies and procedures
4. Perform regular activity reviews, including various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports. The goal of information technology activity review is to prevent, detect, contain, and correct security and/or privacy violations and threats to individually identifiable health information, whether in electronic or any other forms. All information system activity review audits and monitors are routinely performed and documented

The audits, monitors and reviews will focus on the organization's compliance with specific rules and areas that have been the focus of particular attention on the part of the federal Office for Civil Rights (OCR), which enforces HIPAA <*include the name of state agencies if applicable*>. The privacy and security officer(s) shall supervise all auditing and monitoring under privacy and security compliance programs. The organization recognizes that privacy and security are intertwined and codependent, resulting in an interdepartmental, enterprise-wide approach to both privacy and security compliance programs, policies and procedures. Additionally, the privacy and security officer(s) shall maintain all reports, documents and written materials created by the ongoing monitoring, including reports of suspected noncompliance.

Techniques

Audit techniques may include, but are not limited to:

1. Personnel interviews.
2. General questionnaires submitted to Employees and Contractors;
3. Reviews of OCR privacy and /or security complaints;
4. Other electronic health record (EHR) system audit log monitoring for unauthorized PHI access, use, or disclosure.
5. Request and review all BA records to ensure privacy and security compliance per business associate agreement (BAA).

Operational Privacy and Security Monitor and Audit Topics

The topics of operational privacy and security monitoring audits can vary according to perceived needs, complaints or routine proactive vigilance. Below are a list of topics that can be audited for privacy, each audit requiring its own design and configuration according to the organization's policies and procedures. Newer HIPAA topics such as breach determination and notification should be factored into current audit plans.

1. Individual (Patient) Rights
    a. Notice of privacy practice forms completion at pre-registration or registration and follow-up on changes or restrictions documented
        i. NPP posted
    b. Patient access to their own (or otherwise authorized) PHI
        i. Properly completed authorization(s)
        ii. Proper ID and supporting documentation presented
        iii. Electronic record access for individuals (patients)
        iv. Electronic record mandated copies for individuals (patients)
    c. Patient Amendment to PHI
        i. Properly executed form
        ii. Physician notification process followed
        iii. Denial/rebuttal process
        iv. Were requested elements amended as requested (if allowed)
    d. Restrictions on PHI use being followed (patients can request and must be granted certain restrictions, there are fewer options not to provide restrictions by the CE)
        i. Flags set for notification within registration and other electronic systems to notify workforce members of restrictions
        ii. Securing disclosures of PHI in response to restrictions processes being followed
2. Privacy Event and Determination Investigations
    a. Completion of appropriate forms and logs for privacy events
    b. Proper privacy event and privacy violation (breach determination) procedures followed
    c. Proper individual (patient), the organization and OCR notifications
3. Workforce Member Privacy Training
    a. Training privacy procedures being followed, at new hire (volunteer or other) orientation
    b. Routine, periodic privacy training being accomplished on schedule and with correct materials

4. Workforce Member PHI Use, Access and Disclosure
    a. Log in attempts and log ins, with locations if possible
    b. Is access level to PHI in electronic systems appropriate (examples below):
        i. Users who accessed a defined patient
        ii. Access by device
        iii. All patients accessed by a defined user
        iv. Access to defined user/patient
        v. All access for a period of time
        vi. Access by application
        vii. Same last name match user/patient
        viii. Same street match user/patient
        ix. Patients and CE employee match
        x. User/patient location match
        xi. Discharged patients
        xii. Patient Provider match
        xiii. Excessive session duration match
        xiv. VIP/Confidential match
        xv. Total time per device/application
    c. Was access to systems (de-provisioning) with PHI removed within one day?
    d. Were devices containing PHI returned to the organization within one day of termination?
        i. Are appropriate records kept for these activities?
    e. Are print permissions appropriate?
        i. Print copies by user
        ii. Print times by user
        iii. User printing by devices
        iv. Actual documents printed
    f. Audit log reviews of PHI access, use and disclosure
    g. Release of information logs and appropriate disclosure of PHI by workforce members
    h. Secure messaging/e-mail disclosure audits
    i. Electronic copies for disclosure audits, who, what, when, and to which requesting parties
    j. Fax logs and misdirected fax detection
    k. Auto fax number integrity

5. Fields helpful to capture privacy and security auditing (both manual and automated) may include, but not limited to the following:
   a. Account number
   b. EMPI number
   c. Medical record number
   d. Confidential patient flag
   e. Discharge date
   f. Employee department
   g. Employee match
   h. Facility
   i. Guarantor name
   j. Location match
   k. Patient address (main)
   l. Patient address (additional)
   m. Patient location
   n. Patient name
   o. Patient ZIP code
   p. Procedure
   q. Provider match
   r. Session start date and time
   s. Session stop date and time
   t. Print by user and device

Documentation of Privacy Compliance Efforts

The organization should document its efforts to comply with applicable statutes, regulations, guidelines and federal and state healthcare privacy and security program requirements. For example, when the organization, in its efforts to comply with a particular statute, regulation, guideline, or program requirement, requests advice from a government agency, including OCR, the organization shall document and maintain a record of the request and any written or oral response. Additionally, the organization shall maintain a log of all inquiries between its workforce members and any third parties, as well as any records relevant to issues where the organization relies upon the reasonableness of any responses it receives from a state or federal healthcare privacy or security program or agency. This procedure is extremely important for the organization in order for it to rely upon such responses and to guide it in future decisions, actions or appeals.

Privacy and Security Officer Function

The privacy and/or security officer(s), or their designee, shall record the information necessary to conduct an appropriate investigation of all privacy and security complaints.

Reprisal/Retaliation Prohibited

Any threat of reprisal against a person who acts pursuant to his or her responsibilities in relation to privacy and security laws, rules, and regulations is not only against the Organization's policy, it may in some instances be a violation of the law. Reprisal, if proven, shall be subject to appropriate disciplinary action.

False Reports/Discipline

It is the policy of the organization that no workforce member will be punished solely on the basis that they reported what was reasonably believed to be an act of wrongdoing or a violation of privacy or security. However, a workforce member will be subject to disciplinary action if the organization reasonably concludes that the workforce member knowingly made a false allegation, or knowingly distorted, exaggerated, or minimized an incident to either injure someone else or to protect the workforce member or others. Any attempt to harm or slander another person through false accusations, malicious rumors, or other irresponsible actions is a violation of the organization's policy.

Anonymity

The organization, at the request of a reporting workforce member, shall provide anonymity to the workforce member who reports the privacy or security event or suspected violation as is possible under the circumstances in the judgment of the privacy or security officer, consistent with the organization's obligation to investigate concerns and take necessary corrective action.

Admissions of Wrongdoing

An admission of personal wrongdoing will not guarantee that a workforce member will be protected from disciplinary action. The weight to be given to the admission in determining whether a workforce member will be disciplined will depend on all the facts known to the organization at the time. An admission of wrongdoing will be taken into account if the organization was not previously aware of the reporting workforce member's conduct, or its discovery was not imminent, and if the admission was complete and truthful.

E. Related procedures

<Insert appropriate procedures and descriptions of technologies used for auditing and monitoring>

F. Related Policies

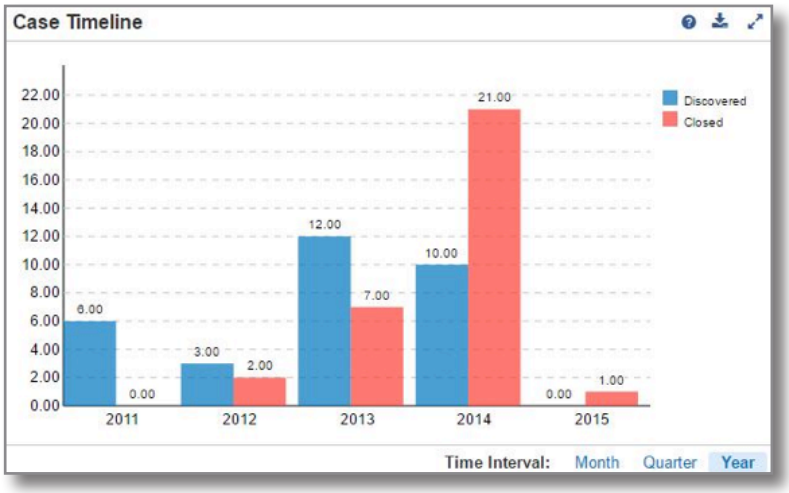
- 6s–Appropriate access to PHI by workforce
- Mitigation for improper use or disclosure of PHI
- 26s–Sanctions, Enforcement and discipline
- 106s–Log in monitoring

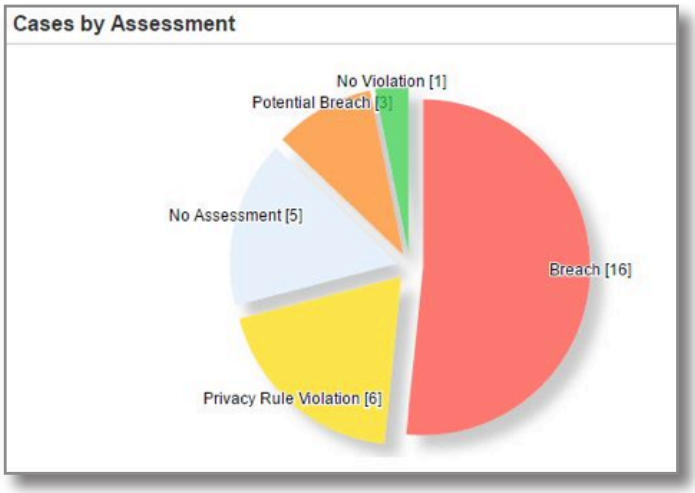
G. References

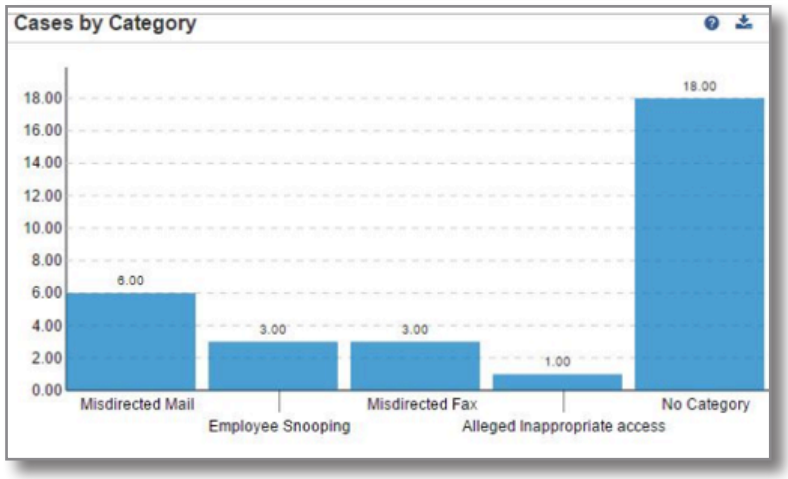
- Title 45, Code of Federal Regulations, Parts 160 and 164, August 14, 2002.
- 45 CFR 164.524, §164.312(b)
- 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule
- SRA Line Item Numbers: B14, B15, B16, B22, B33, B42, B43, B65, B96, C2, D5, D17,D18, D19, D20

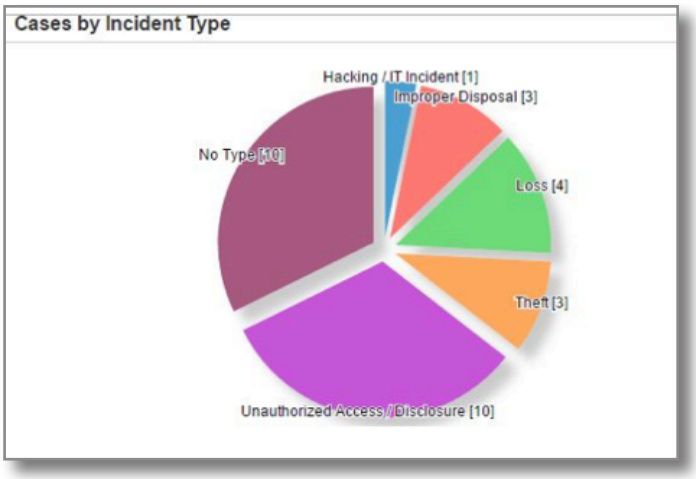
APPENDIX H

SAMPLE HIPAA REPORTING DASHBOARD









0	0	31	282
New Cases	Active Cases	Closed Cases	Avg # of Days Open