Compliancy Group

From Panicked to Prepared: How to Reply to a HIPAA Audit

MISSION

→ We simplify compliance so you can confidently grow your business

VISION

→ To be the affordable industry standard for simplified compliance

VALUES

→ Accountability, Grit, Integrity, Focus

THE HISTORY OF Compliancy Group

2005
Compliancy Group was founded

The Guard
Total HIPAA Compliance Solution
Achieve, Illustrate, Maintain Methodology

Proven Methodology
No client has failed an OCR/CMS audit ever!
Thousands of clients throughout the US & other countries
Compliance Coaching Support

2023
Recognized HIPAA Leaders
Endorsed or Preferred by over 50 Medical Associations

Awards, Endorsements, & Partners

Introduction to HIPAA Compliance

The 7 Fundamentals Elements of an Effective Compliance Program

1. Implement written policies, procedures, and standards of conduct
2. Designate a person to ensure they are followed
3. Conduct effective training and education
4. Develop effective lines of communication
5. Conduct internal monitoring and auditing
6. Enforce standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective auction

Four HIPAA Rules

Privacy Rule

Use & Disclosure Requirements. Provides individuals with a legal and enforceable right to see and receive copies of their medical and other health records upon request provided by their health care providers and health plans.

Security Rule

Establishes standards to protect ePHI that is created, received, used, or maintained by a covered entity. Also requires administrative, physical, & technical safeguards to ensure the confidentiality, integrity, and security of ePHI.

Omnibus Rule

Expands the definition of a "Business Associate" to include all entities that create, receive, maintain, or transmit PHI on behalf of a Covered Entity.

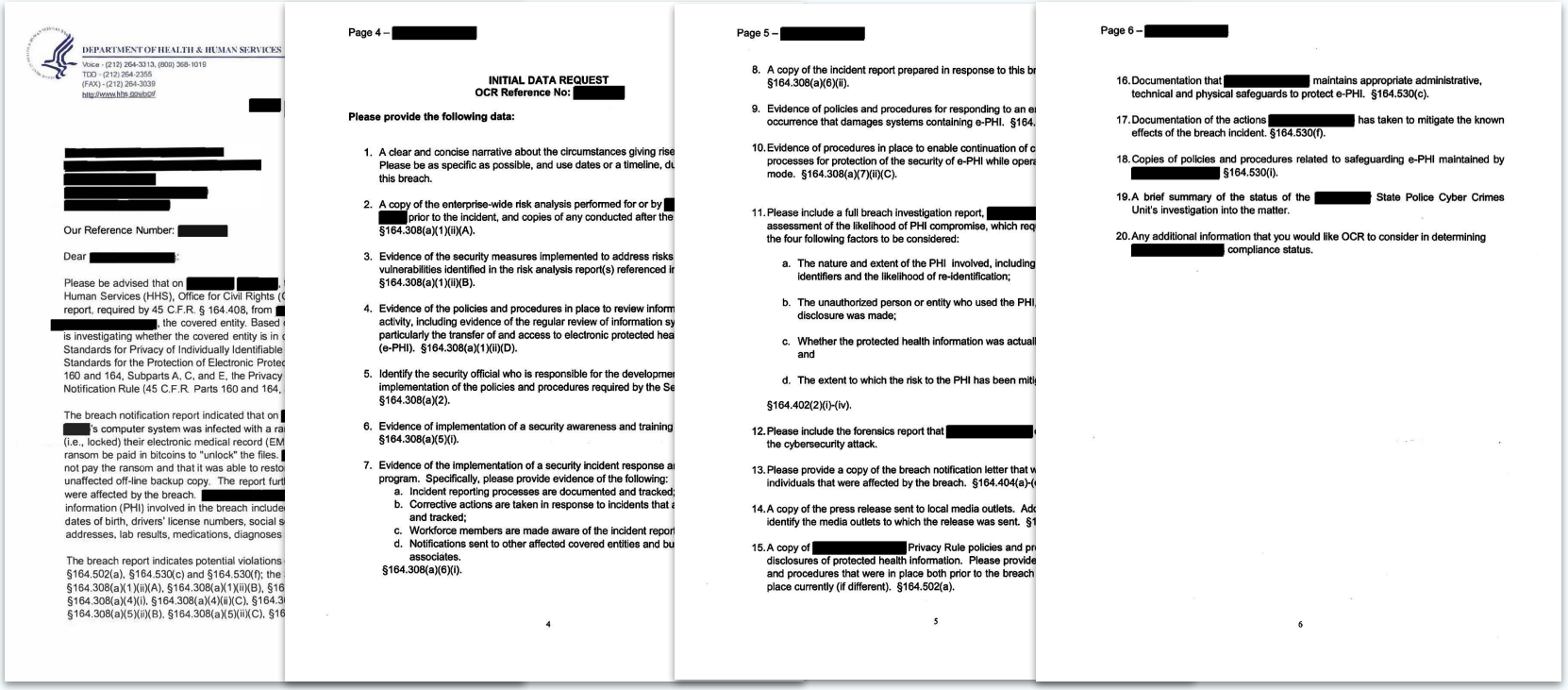
Breach Notification

Requires HIPAA covered entities & their business associates to provide notification following a breach of unsecured PHI. If a breach effects more than 500 people, the Secretary must be notified in no more than 60 days. Less than 500 people can be reported on an annual basis.

HIPAA Lite vs HIPAA Done Right

So You've Been Audited by the OCR

How Do You Know You've Been Audited?



DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (212) 264-3313, (800) 368-1019
TDD - (212) 264-2355
(FAX) - (212) 264-3039
http://www.hhs.gov/ocr/

[redacted]

Our Reference Number: [redacted]

Dear [redacted]:

Please be advised that on [redacted] Human Services (HHS), Office for Civil Rights (O report, required by 45 C.F.R. § 164.408, from [redacted], the covered entity. Based is investigating whether the covered entity is in Standards for Privacy of Individually Identifiable Standards for the Protection of Electronic Protec 160 and 164, Subparts A, C, and E, the Privacy Notification Rule (45 C.F.R. Parts 160 and 164.

The breach notification report indicated that on [redacted]'s computer system was infected with a ra (i.e., locked) their electronic medical record (EM ransom be paid in bitcoins to "unlock" the files. not pay the ransom and that it was able to resto unaffected off-line backup copy. The report furt were affected by the breach. [redacted] information (PHI) involved in the breach include dates of birth, drivers' license numbers, social s addresses, lab results, medications, diagnoses

The breach report indicates potential violations §164.502(a), §164.530(c) and §164.530(f); the §164.308(a)(1)(ii)(A), §164.308(a)(1)(ii)(B), §16 §164.308(a)(4)(i), §164.308(a)(4)(ii)(C), §164.3 §164.308(a)(5)(ii)(B), §164.308(a)(5)(ii)(C), §16

Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumstances giving rise Please be as specific as possible, and use dates or a timeline, du this breach.
2. A copy of the enterprise-wide risk analysis performed for or by [redacted] prior to the incident, and copies of any conducted after the §164.308(a)(1)(ii)(A).
3. Evidence of the security measures implemented to address risks vulnerabilities identified in the risk analysis report(s) referenced i §164.308(a)(1)(ii)(B).
4. Evidence of the policies and procedures in place to review inform activity, including evidence of the regular review of information sy particularly the transfer of and access to electronic protected hea (e-PHI). §164.308(a)(1)(ii)(D).
5. Identify the security official who is responsible for the developmer implementation of the policies and procedures required by the Se §164.308(a)(2).
6. Evidence of implementation of a security awareness and training §164.308(a)(5)(i).
7. Evidence of the implementation of a security incident response a program. Specifically, please provide evidence of the following:
   a. Incident reporting processes are documented and tracked;
   b. Corrective actions are taken in response to incidents that a and tracked;
   c. Workforce members are made aware of the incident report
   d. Notifications sent to other affected covered entities and bu associates.

   §164.308(a)(6)(i).

4

Page 5 – [redacted]

8. A copy of the incident report prepared in response to this br §164.308(a)(6)(ii).
9. Evidence of policies and procedures for responding to an e occurrence that damages systems containing e-PHI. §164.
10. Evidence of procedures in place to enable continuation of c processes for protection of the security of e-PHI while opera mode. §164.308(a)(7)(ii)(C).
11. Please include a full breach investigation report, [redacted] assessment of the likelihood of PHI compromise, which req the four following factors to be considered:
    a. The nature and extent of the PHI involved, including identifiers and the likelihood of re-identification;
    b. The unauthorized person or entity who used the PHI disclosure was made;
    c. Whether the protected health information was actual and
    d. The extent to which the risk to the PHI has been miti

    §164.402(2)(i)-(iv).
12. Please include the forensics report that [redacted] the cybersecurity attack.
13. Please provide a copy of the breach notification letter that w individuals that were affected by the breach. §164.404(a)-(
14. A copy of the press release sent to local media outlets. Ad identify the media outlets to which the release was sent. §1
15. A copy of [redacted] Privacy Rule policies and pr disclosures of protected health information. Please provide and procedures that were in place both prior to the breach place currently (if different). §164.502(a).

5

Page 6 – [redacted]

16. Documentation that [redacted] maintains appropriate administrative, technical and physical safeguards to protect e-PHI. §164.530(c).
17. Documentation of the actions [redacted] has taken to mitigate the known effects of the breach incident. §164.530(f).
18. Copies of policies and procedures related to safeguarding e-PHI maintained by [redacted] §164.530(i).
19. A brief summary of the status of the [redacted] State Police Cyber Crimes Unit's investigation into the matter.
20. Any additional information that you would like OCR to consider in determining [redacted] compliance status.

6

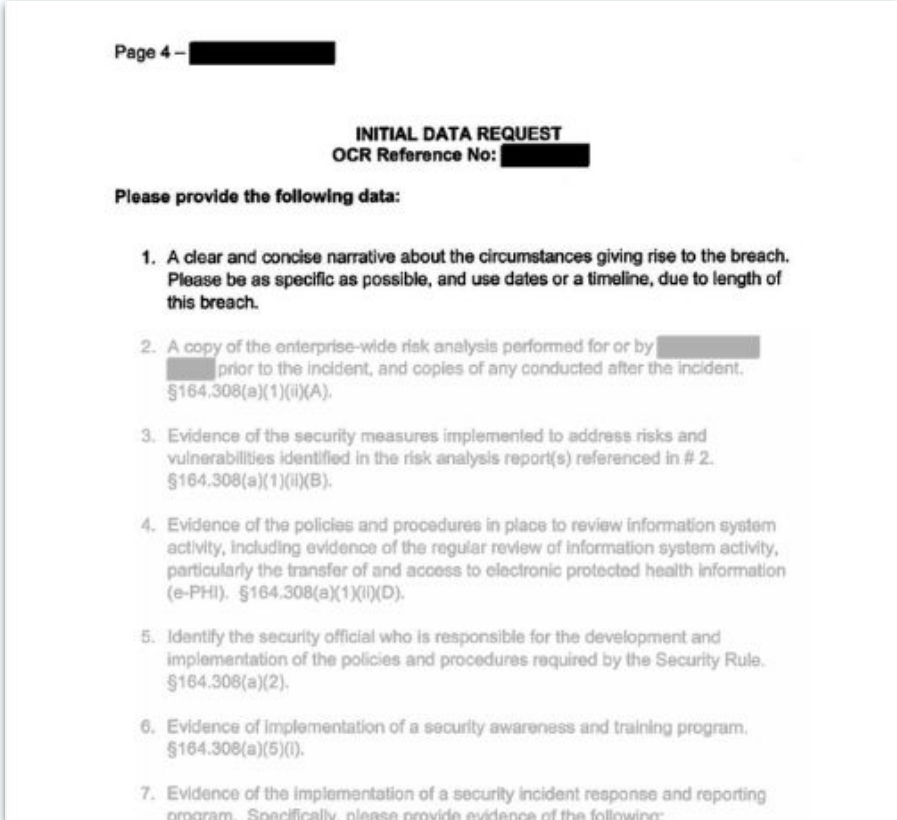
Your first notification of an audit will always come via written letter in the mail

What is the OCR?

The U.S. Department of Health and Human Services (HHS) **Office for Civil Rights (OCR)** enforces federal civil rights laws, conscience and religious freedom laws, the **Health Insurance Portability and Accountability Act** Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule...

What causes a HIPAA Audit?

1. Patient Complaint
2. Employee Whistleblower
3. Reportable Breach (ie. Ransomware, theft, etc).



Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumstances giving rise to the breach. Please be as specific as possible, and use dates or a timeline, due to length of this breach.
2. A copy of the enterprise-wide risk analysis performed for or by [redacted] prior to the incident, and copies of any conducted after the incident. §164.308(a)(1)(ii)(A).
3. Evidence of the security measures implemented to address risks and vulnerabilities identified in the risk analysis report(s) referenced in # 2. §164.308(a)(1)(ii)(B).
4. Evidence of the policies and procedures in place to review information system activity, including evidence of the regular review of information system activity, particularly the transfer of and access to electronic protected health information (e-PHI). §164.308(a)(1)(ii)(D).
5. Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule. §164.308(a)(2).
6. Evidence of implementation of a security awareness and training program. §164.308(a)(5)(i).
7. Evidence of the implementation of a security incident response and reporting program. Specifically, please provide evidence of the following:

Step 1: Don’t Panic!

The purpose of an Audit is:

1. For the OCR to **review** and **analyze** your documentation

2. The results **help** the OCR to better understand where you stand in regards to the HIPAA rules, to provide guidance and a corrective action plan when needed.

Step 2: Understand Why You've Been Audited

1.

Was a **complaint** filed against the practice by a **patient** or **internal whistleblower?**

2.

Was a **breach reported** to the Office for Civil Rights?

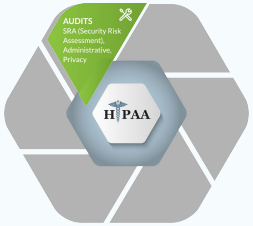
Step 3: Don’t Miss a Step In Your Reply

1. Be **prepared** ahead of time. Do you have a compliance solution, legal representation, or cyber liability insurance coverage? You don’t want to do this alone!

2. Respond within **10 business days** - responding last minute can indicate a deficiency

3. **Send only what is requested** and be honest about any gaps.

How to Reply to an OCR Audit



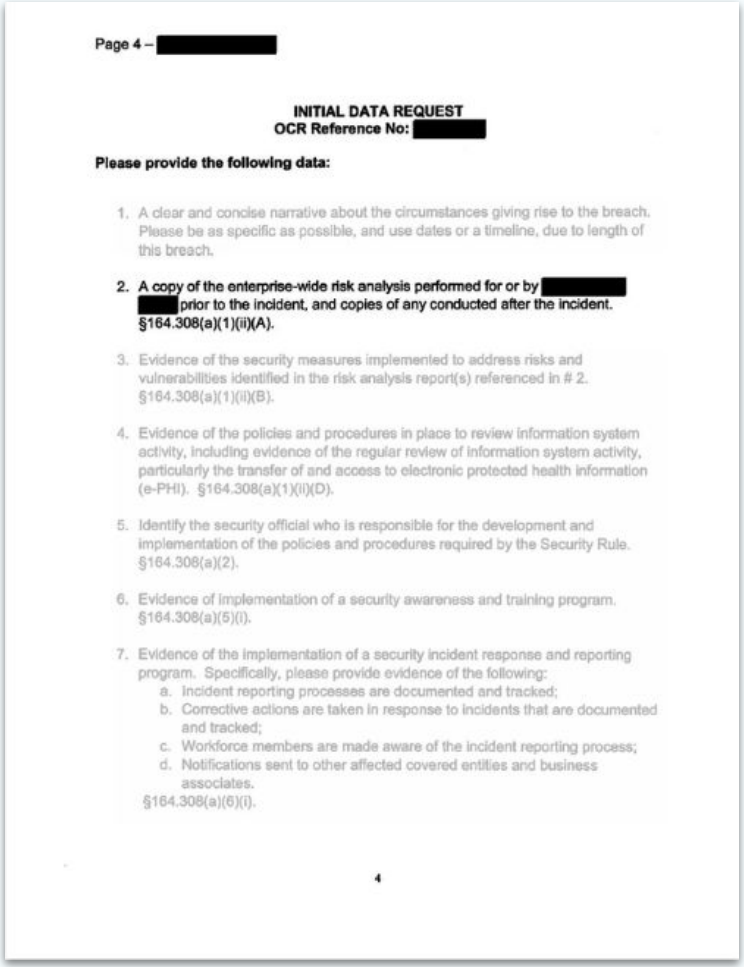
Risk Assessment

What Does This Mean?

The OCR is asking you for proof of an **ongoing** Security Risk Analysis*

*The Risk Analysis is there to help your organization ensure its compliance with HIPAA's administrative, physical, and technical safeguards

*The Risk Analysis is also there to expose any gaps that protected health information may be at risk, so your practice can illustrate **"Good Faith Effort"**



Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumstances giving rise to the breach. Please be as specific as possible, and use dates or a timeline, due to length of this breach.

2. **A copy of the enterprise-wide risk analysis performed for or by [redacted] prior to the incident, and copies of any conducted after the incident. §164.308(a)(1)(ii)(A).**

3. Evidence of the security measures implemented to address risks and vulnerabilities identified in the risk analysis report(s) referenced in # 2. §164.308(a)(1)(ii)(B).

4. Evidence of the policies and procedures in place to review information system activity, including evidence of the regular review of information system activity, particularly the transfer of and access to electronic protected health information (e-PHI). §164.308(a)(1)(ii)(D).

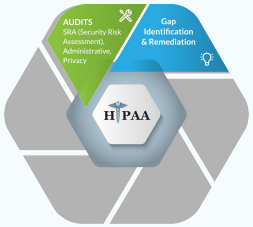
5. Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule. §164.308(a)(2).

6. Evidence of implementation of a security awareness and training program. §164.308(a)(5)(i).

7. Evidence of the implementation of a security incident response and reporting program. Specifically, please provide evidence of the following:
   a. Incident reporting processes are documented and tracked;
   b. Corrective actions are taken in response to incidents that are documented and tracked;
   c. Workforce members are made aware of the incident reporting process;
   d. Notifications sent to other affected covered entities and business associates.

   §164.308(a)(6)(i).

4



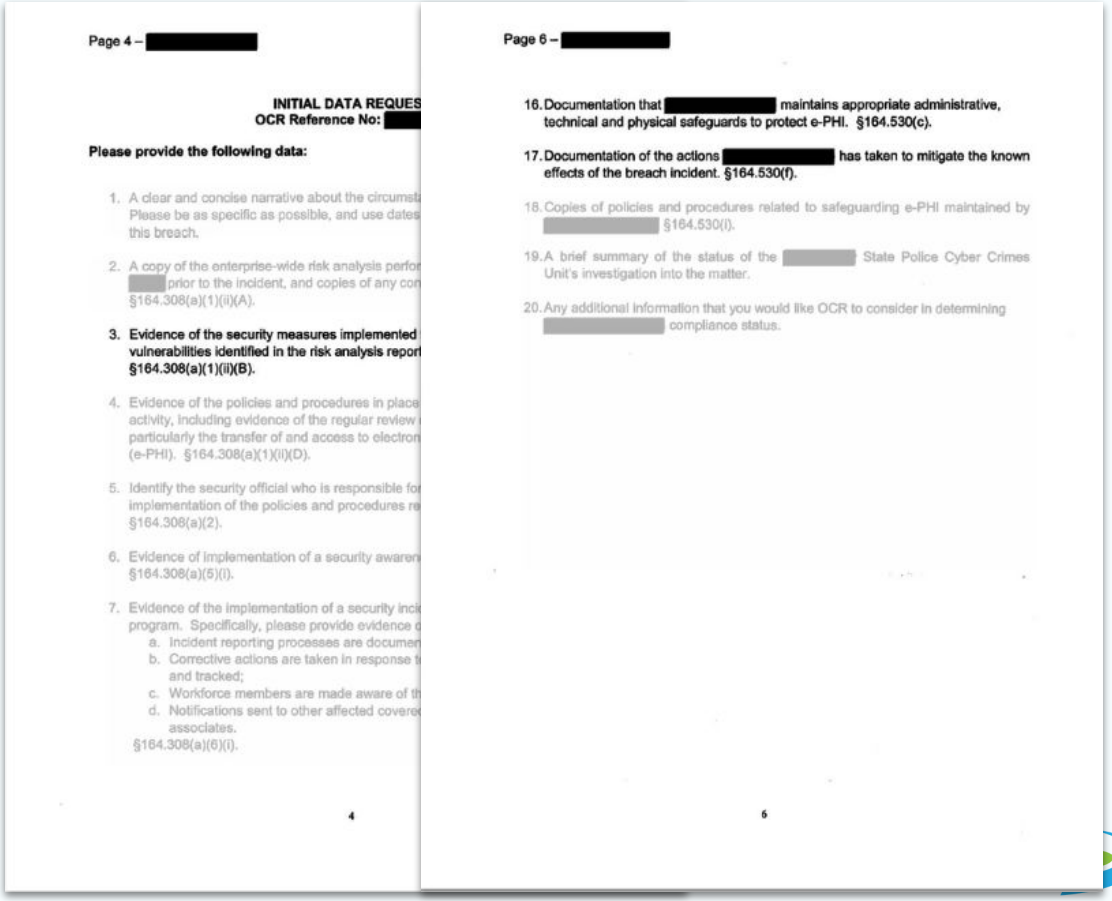
Gap Identification & Remediation

What Does This Mean?

The OCR is asking for documentation relating to how an entity closed the gaps that were found following a completed Security Risk Analysis*

*Compliance / Remediation Plans refer to the organized efforts documented to ensure closure of identified gaps uncovered.

<u>If it isn't documented…. It's not happening.</u>



Page 4 – [redacted]

INITIAL DATA REQUES
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumst
Please be as specific as possible, and use dates
this breach.

2. A copy of the enterprise-wide risk analysis perfor
[redacted] prior to the incident, and copies of any cor
§164.308(a)(1)(ii)(A).

3. **Evidence of the security measures implemented
vulnerabilities identified in the risk analysis repor
§164.308(a)(1)(ii)(B).**

4. Evidence of the policies and procedures in place
activity, including evidence of the regular review
particularly the transfer of and access to electron
(e-PHI). §164.308(a)(1)(ii)(D).

5. Identify the security official who is responsible fo
implementation of the policies and procedures re
§164.308(a)(2).

6. Evidence of implementation of a security awaren
§164.308(a)(5)(i).

7. Evidence of the implementation of a security inci
program. Specifically, please provide evidence
a. Incident reporting processes are documen
b. Corrective actions are taken in response t
and tracked;
c. Workforce members are made aware of th
d. Notifications sent to other affected covere
associates.
§164.308(a)(6)(i).

4

Page 6 – [redacted]

16. Documentation that [redacted] maintains appropriate administrative, technical and physical safeguards to protect e-PHI. §164.530(c).

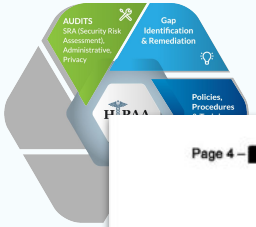
17. Documentation of the actions [redacted] has taken to mitigate the known effects of the breach incident. §164.530(f).

18. Copies of policies and procedures related to safeguarding e-PHI maintained by [redacted] §164.530(i).

19. A brief summary of the status of the [redacted] State Police Cyber Crimes Unit's investigation into the matter.

20. Any additional information that you would like OCR to consider in determining [redacted] compliance status.

6



Policies, Procedures, & Training

Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumstances giving r
Please be as specific as possible, and use dates or a timeline,
this breach.

2. A copy of the enterprise-wide risk analysis performed for or by
[redacted] prior to the incident, and copies of any conducted after t
§164.308(a)(1)(ii)(A).

3. Evidence of the security measures implemented to address ris
vulnerabilities identified in the risk analysis report(s) reference
§164.308(a)(1)(ii)(B).

4. **Evidence of the policies and procedures in place to review info**
activity, including evidence of the regular review of information
particularly the transfer of and access to electronic protected h
(e-PHI). §164.308(a)(1)(ii)(D).

5. Identify the security official who is responsible for the develop
implementation of the policies and procedures required by the
§164.308(a)(2).

6. **Evidence of implementation of a security awareness and traini**
§164.308(a)(5)(i).

7. Evidence of the implementation of a security incident response
program. Specifically, please provide evidence of the following
   a. Incident reporting processes are documented and tracke
   b. Corrective actions are taken in response to incidents th
   and tracked;
   c. Workforce members are made aware of the incident rep
   d. Notifications sent to other affected covered entities and
   associates.

§164.308(a)(6)(i).

4

Page 5 – [redacted]

8. A copy of the incident report prepared in response to this breach.
§164.308(a)(6)(ii).

9. **Evidence of policies and procedures for responding to an emergency or ot**
occurrence that damages systems containing e-PHI. §164.308(a)(7)(i).

10. **Evidence of procedures in place to enable continuation of critical business**
processes for protection of the security of e-PHI while operating in emerge
mode. §164.308(a)(7)(ii)(C).

11. Please include a full breach investigation report, [redacted]
assessment of the likelihood of PHI compromise, which requires, at a mini
the four following factors to be considered:

   a. The nature and extent of the PHI involved, including the types of
   identifiers and the likelihood of re-identification;

   b. The unauthorized person or entity who used the PHI, or to whom th
   disclosure was made;

   c. Whether the protected health information was actually acquired or
   and

   d. The extent to which the risk to the PHI has been mitigated.

§164.402(2)(i)-(iv).

12. Please include the forensics report that [redacted] obtained as a r
the cybersecurity attack.

13. Please provide a copy of the breach notification letter that was sent to the
individuals that were affected by the breach. §164.404(a)-(d).

14. A copy of the press release sent to local media outlets. Additionally, pleas
identify the media outlets to which the release was sent. §164.404(a)-(c).

15. **A copy of [redacted] Privacy Rule policies and procedures on us**
disclosures of protected health information. Please provide copies of the
and procedures that were in place both prior to the breach incident, and t
place currently (if different). §164.502(a).

5

Page 6 – [redacted]

16. Documentation that [redacted] maintains appropriate administrative,
technical and physical safeguards to protect e-PHI. §164.530(c).

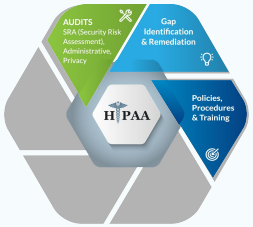
17. Documentation of the actions [redacted] has taken to mitigate the known
effects of the breach incident. §164.530(f).

18. **Copies of policies and procedures related to safeguarding e-PHI maintained by**
[redacted] §164.530(i).

19. A brief summary of the status of the [redacted] State Police Cyber Crimes
Unit's investigation into the matter.

20. Any additional information that you would like OCR to consider in determining
[redacted] compliance status.

6

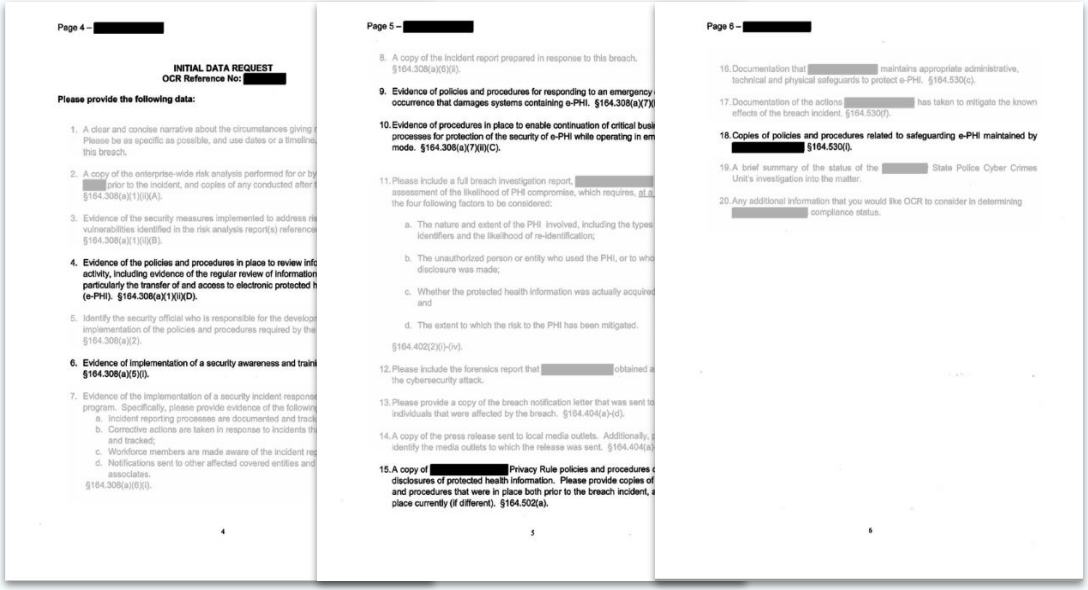


Policies, Procedures, & Training

What Does This Mean?

HIPAA Policies and Procedures are a set of standards that all must follow to ensure private information is protected.

Training ensures all employees are up to date on what steps to take to guarantee the privacy and security of protected health information (PHI).



Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumstances giving r
Please be as specific as possible, and use dates or a timeline
this breach.
2. A copy of the enterprise-wide risk analysis performed for or by
[redacted] prior to the incident, and copies of any conducted after t
§164.308(a)(1)(ii)(A).
3. Evidence of the security measures implemented to address ris
vulnerabilities identified in the risk analysis report(s) reference
§164.308(a)(1)(ii)(B).
4. **Evidence of the policies and procedures in place to review infl**
activity, including evidence of the regular review of information
particularly the transfer of and access to electronic protected h
(e-PHI). §164.308(a)(1)(ii)(D).
5. Identify the security official who is responsible for the develop
implementation of the policies and procedures required by the
§164.308(a)(2).
6. **Evidence of implementation of a security awareness and traini**
§164.308(a)(5)(i).
7. Evidence of the implementation of a security incident respons
program. Specifically, please provide evidence of the followin
a. Incident reporting processes are documented and track
b. Corrective actions are taken in response to incidents th
and tracked;
c. Workforce members are made aware of the incident re
d. Notifications sent to other affected covered entities and
associates.
§164.308(a)(6)(ii).

4

Page 5 – [redacted]

8. A copy of the incident report prepared in response to this breach.
§164.308(a)(6)(ii).
9. **Evidence of policies and procedures for responding to an emergency**
occurrence that damages systems containing e-PHI. §164.308(a)(7)(
10. **Evidence of procedures in place to enable continuation of critical busi**
processes for protection of the security of e-PHI while operating in em
mode. §164.308(a)(7)(ii)(C).
11. Please include a full breach investigation report, [redacted]
assessment of the likelihood of PHI compromise, which requires, at a
the four following factors to be considered:
a. The nature and extent of the PHI involved, including the types
identifiers and the likelihood of re-identification;
b. The unauthorized person or entity who used the PHI, or to who
disclosure was made;
c. Whether the protected health information was actually acquire
and
d. The extent to which the risk to the PHI has been mitigated.
§164.402(2)(i)-(iv).
12. Please include the forensics report that [redacted] obtained a
the cybersecurity attack.
13. Please provide a copy of the breach notification letter that was sent to
individuals that were affected by the breach. §164.404(a)-(d).
14. A copy of the press release sent to local media outlets. Additionally,
identify the media outlets to which the release was sent. §164.404(a)
15. **A copy of [redacted] Privacy Rule policies and procedures**
disclosures of protected health information. Please provide copies of
and procedures that were in place both prior to the breach incident, a
place currently (if different). §164.502(a).

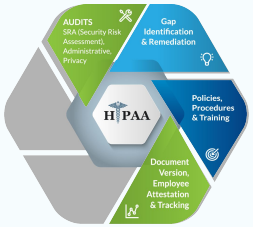
5

Page 6 – [redacted]

16. Documentation that [redacted] maintains appropriate administrative,
technical and physical safeguards to protect e-PHI. §164.530(c).
17. Documentation of the actions [redacted] has taken to mitigate the known
effects of the breach incident. §164.530(f).
18. **Copies of policies and procedures related to safeguarding e-PHI maintained by**
[redacted] §164.530(i).
19. A brief summary of the status of the [redacted] State Police Cyber Crimes
Unit's investigation into the matter.
20. Any additional information that you would like OCR to consider in determining
[redacted] compliance status.

6

Behavioral Health Center of EXCELLENCE

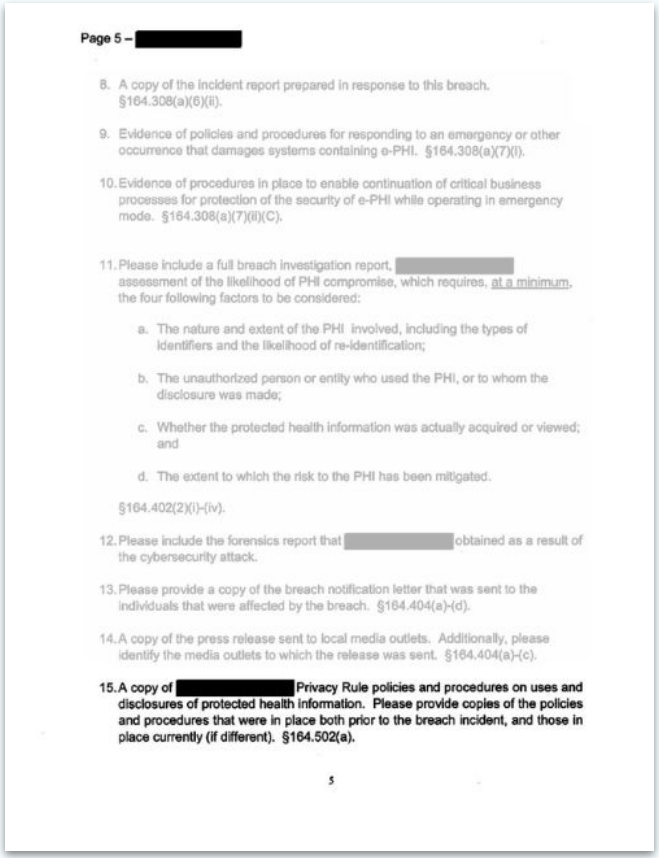


Document Version*, Employee Attestation & Tracking

What Does This Mean?

More than simply having policies, the OCR wants to ensure that staff is being trained on those policies, is following the policies, and that they are being tracked and updated as needed.

***Document Version** assists you in the event the OCR is asking you for policies in place at the time of a specific incident.



Page 5 – [redacted]

8. A copy of the incident report prepared in response to this breach. §164.308(a)(6)(ii).

9. Evidence of policies and procedures for responding to an emergency or other occurrence that damages systems containing e-PHI. §164.308(a)(7)(i).

10. Evidence of procedures in place to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode. §164.308(a)(7)(ii)(C).

11. Please include a full breach investigation report, [redacted] assessment of the likelihood of PHI compromise, which requires, at a minimum, the four following factors to be considered:

    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

    b. The unauthorized person or entity who used the PHI, or to whom the disclosure was made;

    c. Whether the protected health information was actually acquired or viewed; and

    d. The extent to which the risk to the PHI has been mitigated.

    §164.402(2)(i)-(iv).

12. Please include the forensics report that [redacted] obtained as a result of the cybersecurity attack.

13. Please provide a copy of the breach notification letter that was sent to the individuals that were affected by the breach. §164.404(a)-(d).

14. A copy of the press release sent to local media outlets. Additionally, please identify the media outlets to which the release was sent. §164.404(a)-(c).

15. A copy of [redacted] Privacy Rule policies and procedures on uses and disclosures of protected health information. Please provide copies of the policies and procedures that were in place both prior to the breach incident, and those in place currently (if different). §164.502(a).

5

Incident Management

Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. **A clear and concise narrative about the circumstances g**
   Please be as specific as possible, and use dates or a tir
   this breach.
2. A copy of the enterprise-wide risk analysis performed fo
   [redacted] prior to the incident, and copies of any conducted
   §164.308(a)(1)(ii)(A).
3. Evidence of the security measures implemented to addr
   vulnerabilities identified in the risk analysis report(s) refe
   §164.308(a)(1)(ii)(B).
4. Evidence of the policies and procedures in place to revi
   activity, including evidence of the regular review of infor
   particularly the transfer of and access to electronic prote
   (e-PHI). §164.308(a)(1)(ii)(D).
5. Identify the security official who is responsible for the de
   implementation of the policies and procedures required
   §164.308(a)(2).
6. Evidence of implementation of a security awareness and
   §164.308(a)(5)(i).
7. **Evidence of the implementation of a security incident re**
   program. Specifically, please provide evidence of the fo
   a. Incident reporting processes are documented and
   b. Corrective actions are taken in response to incide
   and tracked;
   c. Workforce members are made aware of the incid
   d. Notifications sent to other affected covered entitie
   associates.
   §164.308(a)(6)(i).

4

Page 5 – [redacted]

8. **A copy of the incident report prepared in response to this bre**
   §164.308(a)(6)(ii).
9. Evidence of policies and procedures for responding to an em
   occurrence that damages systems containing e-PHI. §164.3
10. Evidence of procedures in place to enable continuation of cri
    processes for protection of the security of e-PHI while operat
    mode. §164.308(a)(7)(ii)(C).
11. **Please include a full breach investigation report, [redacted]**
    assessment of the likelihood of PHI compromise, which requi
    the four following factors to be considered:
    a. The nature and extent of the PHI involved, including t
    identifiers and the likelihood of re-identification;
    b. The unauthorized person or entity who used the PHI, c
    disclosure was made;
    c. Whether the protected health information was actually
    and
    d. The extent to which the risk to the PHI has been mitiga
    §164.402(2)(i)-(iv).
12. **Please include the forensics report that [redacted] ob**
    the cybersecurity attack.
13. **Please provide a copy of the breach notification letter that wa**
    individuals that were affected by the breach. §164.404(a)-(d)
14. **A copy of the press release sent to local media outlets. Addit**
    identify the media outlets to which the release was sent. §16
15. A copy of [redacted] Privacy Rule policies and proc
    disclosures of protected health information. Please provide
    and procedures that were in place both prior to the breach i
    place currently (if different). §164.502(a).

5

Page 6 – [redacted]

16. Documentation that [redacted] maintains appropriate administrative, technical and physical safeguards to protect e-PHI. §164.530(c).
17. Documentation of the actions [redacted] has taken to mitigate the known effects of the breach incident. §164.530(f).
18. Copies of policies and procedures related to safeguarding e-PHI maintained by [redacted] §164.530(i).
19. **A brief summary of the status of the [redacted] State Police Cyber Crimes Unit's investigation into the matter.**
20. Any additional information that you would like OCR to consider in determining [redacted] compliance status.

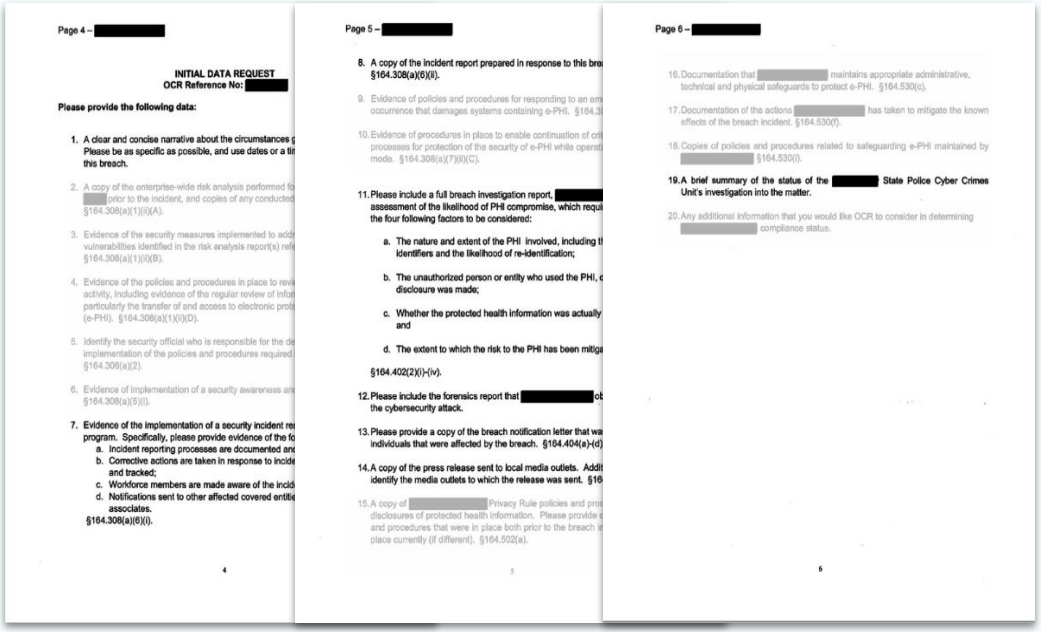
6

Incident Management

What Does This Mean?

HIPAA requires Covered Entities to develop an incident log, breach determination, investigation, and response plan. CE's must have a data backup plan, a disaster recovery plan, an emergency mode operation plan, and other administrative safeguards.

Breach reporting requirements vary depending on the size, scope, and nature of the breach.



Page 4 – [redacted]

INITIAL DATA REQUEST
OCR Reference No: [redacted]

Please provide the following data:

1. A clear and concise narrative about the circumstances
Please be as specific as possible, and use dates or a ti
this breach.
2. A copy of the enterprise-wide risk analysis performed fo
prior to the incident, and copies of any conducted
§164.308(a)(1)(ii)(A).
3. Evidence of the security measures implemented to add
vulnerabilities identified in the risk analysis report(s) refe
§164.308(a)(1)(ii)(B).
4. Evidence of the policies and procedures in place to revi
activity, including evidence of the regular review of infor
particularly the transfer of and access to electronic prote
(e-PHI). §164.308(a)(1)(ii)(D).
5. Identify the security official who is responsible for the de
implementation of the policies and procedures required
§164.308(a)(2).
6. Evidence of implementation of a security awareness an
§164.308(a)(5)(i).
7. Evidence of the implementation of a security incident re
program. Specifically, please provide evidence of the fo
a. Incident reporting processes are documented an
b. Corrective actions are taken in response to incid
and tracked;
c. Workforce members are made aware of the incid
d. Notifications sent to other affected covered entiti
associates.
§164.308(a)(6)(i).

4

Page 5 – [redacted]

8. A copy of the incident report prepared in response to this bre
§164.308(a)(6)(ii).
9. Evidence of policies and procedures for responding to an em
occurrence that damages systems containing e-PHI. §164.3
10. Evidence of procedures in place to enable continuation of cri
processes for protection of the security of e-PHI while operati
mode. §164.308(a)(7)(ii)(C).
11. Please include a full breach investigation report, [redacted]
assessment of the likelihood of PHI compromise, which requi
the four following factors to be considered:
a. The nature and extent of the PHI involved, including t
identifiers and the likelihood of re-identification;
b. The unauthorized person or entity who used the PHI, c
disclosure was made;
c. Whether the protected health information was actually
and
d. The extent to which the risk to the PHI has been mitiga
§164.402(2)(i)-(iv).
12. Please include the forensics report that [redacted] ob
the cybersecurity attack.
13. Please provide a copy of the breach notification letter that wa
individuals that were affected by the breach. §164.404(a)-(d)
14. A copy of the press release sent to local media outlets. Addi
identify the media outlets to which the release was sent. §16
15. A copy of [redacted] Privacy Rule policies and proc
disclosures of protected health information. Please provide c
and procedures that were in place both prior to the breach i
place currently (if different). §164.502(a).

5

Page 6 – [redacted]

16. Documentation that [redacted] maintains appropriate administrative, technical and physical safeguards to protect e-PHI. §164.530(c).
17. Documentation of the actions [redacted] has taken to mitigate the known effects of the breach incident. §164.530(f).
18. Copies of policies and procedures related to safeguarding e-PHI maintained by [redacted] §164.530(i).
19. **A brief summary of the status of the [redacted] State Police Cyber Crimes Unit's investigation into the matter.**
20. Any additional information that you would like OCR to consider in determining [redacted] compliance status.

6

So What Happens Now?

The Office for Civil Rights will gather all information from the audit and complete a review.

If the audit contains a **serious compliance violation**, the OCR may initiate a corrective action plan or a monetary penalty.

A list of audited entities or their findings will not be posted **unless** requested by the public (Freedom of Information Act)

Wall of Shame

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Bone & Joint Clinic, S.C.	WI	Healthcare Provider	105094	03/13/2023	Hacking/IT Incident	Network Server
	ZOLL Services LLC	MA	Healthcare Provider	997097	03/10/2023	Hacking/IT Incident	Network Server
	Colquitt Complete Care, LLC	GA	Healthcare Provider	1282	03/10/2023	Hacking/IT Incident	Network Server
	Beacon Health System	IN	Healthcare Provider	3117	03/10/2023	Unauthorized Access/Disclosure	Electronic Medical Record
	Wichita Urology Group, PA ("WUG")	KS	Healthcare Provider	1493	03/08/2023	Hacking/IT Incident	Network Server
	EPIC Management, LLC	CA	Health Plan	1190	03/08/2023	Hacking/IT Incident	Email
	Community Health Centers of Greater Dayton	OH	Healthcare Provider	516	03/08/2023	Unauthorized Access/Disclosure	Email
	The M K Morse Company	OH	Health Plan	1378	03/08/2023	Hacking/IT Incident	Network Server
	Trinity Health	MI	Business Associate	45350	03/06/2023	Hacking/IT Incident	Email
	Northeast Surgical Group, PC	MI	Healthcare Provider	15298	03/06/2023	Hacking/IT Incident	Network Server
	West Virginia University Board of Governors	WV	Healthcare Provider	2453	03/03/2023	Unauthorized Access/Disclosure	Network Server
	Denver Public Schools Medical Plans	CO	Health Plan	35068	03/03/2023	Hacking/IT Incident	Network Server

All HIPAA-related breaches of 500+ patients are *public record

HIPAA Fines

Northcutt Dental-Fairhope

$62,500

Impermissible disclosure for marketing, notice of privacy practices, HIPAA Privacy Offer

New England Derm. & Laser Center

$300,640

Improper disposal of PHI, failure to maintain appropriate safeguards, Risk Analysis.

Jacob & Associates

$28,000

Psychiatric Practice. HIPAA Right of Access, Missing HIPAA Policies.

"It should not take a federal investigation before a HIPAA covered entity provides patients, or their personal representatives, with access to their medical records," - OCR Director Lisa J. Pino.

THANK YOU!

Liam Degnan
Director of Strategic Initiatives
(855) 854-4722 Ext. 530
ldegnan@compliancygroup.com