HIPAA Compliance in Home Care

Michael Kern
Kitch Attorneys & Counselors
One Woodward Avenue, Suite 2400
Detroit, MI 48226-5485
313.965.7586
michael.kern@kitch.com
www.kitch.com

KITCH
Attorneys & Counselors
Detroit Lansing Mt. Clemens
Toledo Chicago

Home Care & Hospice

1

Disclaimer

These materials have been prepared by Kitch Attorneys & Counselors PC, for informational purposes only and are not legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel. Photographs, articles, records, pleadings, etc., are for dramatization purposes only.

Home Care & Hospice

2

Topics

HIPAA compliance

- Requirements for health care providers
- Anticipated changes to the Security Rule
- Protecting yourself from a breach

Home Care & Hospice

3

What is HIPAA?

4

Lawsuit against Ascension over data breach affecting 5.6M patients moves forward

Chad Van Alstin | September 24, 2025 | Health Exec | Legal News

A lawsuit against one of the largest nonprofit health systems can move forward, though some claims made by a class action of plaintiffs were dismissed.

The initial complaint was filed in May 2024, shortly after Ascension Health—a Catholic healthcare network with over 90 hospitals in 17 states—was hit by a ransomware attack that exposed records on 5.6 million patients to hackers. The

5

What Is Health Insurance Portability and Accountability Act – HIPAA?

HIPAA is a federal law enacted to:

- Protect the privacy of a patient's personal and health information;
- Provide for electronic and physical security of personal and health information;
- Standardize coding to simplify billing and other transactions.

6

HIPAA

The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996 (HIPAA)

- HIPAA required the U.S. Department of Health and Human Services to develop regulations to protect the privacy and security of certain health information.
  - HITECH
  - Omnibus Rule
  - The HIPAA Privacy Rule.
  - The HIPAA Security Rule.

7

8

What Is HITECH?

- Due to increased privacy and security concerns, the **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth (HITECH) Act was enacted in 2009.
- To promote the adoption and use of health information technology and electronic health records.

9

HITECH Act

HITECH expanded the scope of HIPAA's security and privacy provisions. The changes include:

- Requiring business associates to comply with HIPAA;
- Imposing new notification requirements in the event of a breach of protected health information;
- Strengthening enforcement procedures and penalties;
- Limiting disclosure of protected health information to the minimum necessary to accomplish the intended purpose.

10

What Is the Omnibus Rule?

- "The new rule will help protect patient privacy and safeguard patients' health information in an ever-expanding digital age."
  - HHS Secretary, Kathleen Sebelius
- Implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA.

11

Omnibus Rule – HIPAA HITECH

- Penalties are increased for noncompliance based on the level of negligence.
  - Initially maximum penalty of $1.5 million for a willful violation.
  - Adjusted for inflation, the maximum penalty is now $2.19 million
- Clarified breach notification requirements.
  - When breaches of unsecured health information must be reported to U.S. Dept. of Health & Human Services.
- Individual rights expanded.
  - Patients can ask for their electronic medical record in electronic form.

12

Privacy Rule

- **Requires safeguards** to protect the privacy of personal health information.
- **Sets limits and conditions** on the uses and disclosures that may be made of such information without patient authorization.
- **Gives patients rights** over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

13

Protected Health Information (PHI)

- **Demographic data relating to:**
  - Individual's past, present, or future physical or mental health or condition;
  - The provision of health care to the individual;
  - The past, present, or future payment for the provision of health care to the individual.
- **Anything that identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.**

14

Examples of Common Identifiers

- Name
- Address
- Birth date
- Social security number
- Medical record numbers
- Phone number
- E-mail address
- License numbers
- Photo

15

When to Disclose PHI

- **A Covered Entity may only use or disclose PHI:**
  - With notice to the individual and acknowledgement of how that information will be used ("Notice of Privacy Practices") but only for treatment, payment or healthcare operations (TPO);
  - Without Notice of Privacy Practices under certain circumstances, such as per subpoena, to avert serious threat to health or safety;
  - With a specific written authorization for disclosure for use permitted for other than TPO.
- Even with Notice of Privacy Practices, a Covered Entity must make reasonable efforts to limit use or disclosure of PHI to the "minimum necessary" amount to accomplish the intended purpose of the use or disclosure of PHI.

16

Minimum Necessary Standard

- When HIPAA permits use or disclosure of PHI, a covered entity must use or disclose only the **minimum necessary** PHI required to accomplish the purpose of the use or disclosure.
- The only exceptions to the minimum necessary standard are those times when a covered entity is disclosing PHI for the following reasons:
  - Treatment;
  - Purposes for which an authorization is signed;
  - Disclosures required by law;
  - Sharing information to the patient about himself/herself.

17

HIPAA Forms

- HIPAA compliance documents that you may encounter include
  - Notice of Privacy Practices;
  - Authorization for Use or Disclosure of Information;
  - Business Associate Agreement.

18

Downstream Compliance

- Covered Entity must obtain written "satisfactory assurances" from its direct Business Associate
- Business Associate must obtain written "satisfactory assurances" from its direct Business Associate subcontractor
- Business Associate subcontractor must obtain written "satisfactory assurances" from its direct Business Associate, and so on
- HIPAA Business Associates obligations extend to all downstream subcontractors

19

The Security Rule

- **Establishes** standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
- **Requires** appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

20

The Security Rule

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI
- Specifically, covered entities must:
  1. Ensure the confidentiality, integrity, and availability of all PHI they create, receive, maintain or transmit
  2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
  3. Protect against reasonably anticipated, impermissible uses or disclosures
  4. Ensure compliance by their workforce.

21

Security Rule Compliance

- Directly comply with technical and detailed security standards that apply to Covered Entities:
  - Administrative, physical and technical safeguards
  - Organizational requirements
  - Written policies, procedures and documentation requirements

22

Security Rule Compliance (Cont'd)

- Must develop written security program tailored to organization that describes how the provider will meet each of the standards, safeguards and requirements
- Some standards are required; others are addressable (e.g., encryption)
  - If provider does not implement an addressable standard, it must document why and put in place an equivalent alternative measure

23

Security Rule – Administrative Safeguard Standards

- Administrative Safeguard Standards, e.g.,:
  - Security management process
    - Risk analysis
    - Implement security measure to reduce risks/vulnerabilities (e.g., mobile devices)
    - Apply appropriate sanctions for failure to comply with security policies and procedures
    - Regularly review IS activity, such as audit logs, access reports, and security incident tracking reports (which means you have to do and document these things)

24

Security Rule – Administrative Safeguard Standards (Cont'd)

- Administrative Safeguard Standards, e.g.,:
  - Assign security officer
  - Security awareness and training – security reminders, protection from malicious software, log-in monitoring, password management
  - Security incident procedures – response and reporting
  - Contingency plan
  - Periodic evaluation and updates

25

Security Rule – Physical Safeguard Standards

Physical Safeguard Standards:

- Facility access controls (e.g., locks to restrict access to office and server room)
- Workstation use and security (restrict access to authorized users)
- Device and media controls – policies and procedures re: receipt/removal of hardware and electronic media that contain PHI info, out of and within facility
  - Policies and procedures re: disposal, media re-use, accountability
  - Copiers?

26

Security Rule – Technical Safeguard Standards

Technical Safeguard Standards:

- Basically deal with technological measures to safeguard and control PHI, e.g.,:
  - Access control – e.g., unique user identification, emergency access procedure, automatic logoff
  - Audit controls – hardware, software and/or procedural mechanisms that record and examine activity in IS that contain or use PHI
  - Integrity – Policies and Procedures to protect PHI from improper alteration/destruction
  - Person/entity authentication
  - Transmission security – e.g., encryption

27

Breach Process

28

Breach Defined

- "[A]n acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Rule] is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment."

29

Burden of Proof

- In the event of a breach, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach
  - 45 C.F.R. 164.414

30

Breach Risk Assessment

The Four Factors

1. The nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified
2. The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information
3. Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis
4. The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient

31

Purpose of Security

- To protect the system and information from unauthorized access
- To protect the system and information from unauthorized use.

32

General Security Awareness

- Security (protecting the system and the information it contains) includes protecting against unauthorized access from outside and misuse from within
  - Hardware and software (physical computer systems)
  - Personnel policies
  - Information practice policies
  - Develop disaster/intrusion/response and recovery
  - Designate security responsibilities
  - Develop protocols regarding activities and security at personnel and work station level
  - Safeguards from fire, natural and environmental hazards and intrusions

33

General Security Awareness (Cont'd)

- Two Types of Security with regard to HIPAA:
  1. Building/Physical Security
  2. Computer/Electronic Security

34

Security Has Three Phases

- **Prevention:** Know your risks via risk assessment, protection of data, secure authentication
- **Detection:** Regular monitoring and audits, documentation of these activities
- **Response:** Incident handling response processes, breach notification processes, disciplinary actions (sanctions)

35

PC and System Protection

- Be aware of potential harm
- Follow the e-mail policy; do not click on external links
- Do not download non-approved programs
- Report unknown or suspicious e-mail, attachments

36

Password Management

- What is password security?
  - Do not tell anyone your password
  - Do not write your password down anywhere
  - Change password if others know it
  - Enter your password in private

37

$4.8 million HIPAA Settlement In Data Breach Case

- New York Presbyterian Hospital/Columbia University Medical Center, in their joint arrangement, allegedly disclosed the ePHIs of 6,800 individuals.
- A physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on a network containing NYP patient ePHI.
- Due to lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines.
- Following a complaint by an individual who found an ePHI on the internet, the entities submitted a joint breach report to the OCR.
- Together, the entities paid the OCR a monetary settlement in the amount of $4.8 million and agreed to a corrective action plan including undertaking a risk analysis, developing a risk-management plan, revising policies and procedures, training staff, and providing progress reports

38

QCA Health plan, Inc. Settles for $250,000 in stolen laptop case

- The OCR received a report that an unencrypted laptop computer containing the ePHI of 148 members was stolen from a workforce member's car.
- OCR's investigation revealed that the entity failed to comply with multiple requirements of HIPAA for a period of over 7 years.
- Other than the monetary settlement, QCA has agreed to provide the OCR with an updated risk analysis and a corresponding risk management plan, and to retrain its workforce.

39

Security Rule Update

40

Anticipated changes to the Security Rule

- On January 6, 2025, the HHS Office for Civil Rights published a proposed rule that, if enacted, would significantly change the HIPAA Security Rule.
- The new changes focus on combating cyberattacks and are expected to be finalized by the end of May.
- It is anticipated that providers would be required to implement the changes by end of 2026 or first quarter of 2027.

41

Anticipated changes to the Security Rule (Cont'd)

- New requirements include:
  - Encryption and multi-factor authentication
  - Basic system hardening
  - Backups, business continuity and disaster recovery
  - Incident response planning
  - Access management
- Removes "addressable" distinction for small businesses

42

Encryption and multi-factor authentication

- The new rule includes mandatory encryption of ePHI at rest and in transit and require multi-factor authentication (MFA)
- Providers who do not have encrypted servers should start preparing now
- Phase in MFA for remote access and VPNs

43

Basic system hardening

- The rule requires anti-malware, removal of unnecessary software, and disabling unnecessary network ports for systems that store or process ePHI
- You should start now to ensure you have updated anti-malware systems and that you are removing outdated software

44

Backups, business continuity and disaster recovery

- The new rule has stringent contingency planning requirements:
  - Mandatory written procedures to restore certain systems and data within 72 hours of a service disruption,
  - Separate technical controls for backup and recovery
  - Documented plans for restoration priorities

45

Incident response planning

- The new rule would solidify the need for written incident response plans, workforce reporting procedures, and periodic testing

46

Access management

- The new rule would strengthen access management requirements, including:
  - Notice within 24 hours when a workforce member's access to ePHI or relevant systems is changed or terminated

47

Documentation Considerations

- The new requires that all security policies and procedures must be in writing.
- How to prepare for the change:
  - Initiate a security risk analysis now:
    - Review policies
    - Update your incident response plan
    - Review your back up system
    - Research MFA options

48

HIPAA Breach Case Studies

49

HIPAA Breach #1 – Theft of Laptop

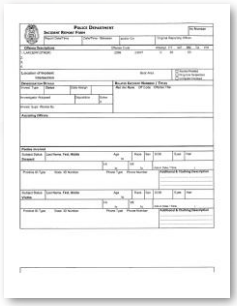
- A criminal broke a window to gain access to a locked office and stole several items, including the unencrypted laptop of a staff member.
- On the stolen laptop were spreadsheets containing the names of residents along with some observations on physical conditions.

50

Risk Assessment

- In order to determine the nature and extent of the protected health information involved, the provider launched an investigation.
  - The provider confirmed that the information on the laptop had information related to 200 patients, including information on resident names, room number, and comments regarding any changes in condition
  - The provider also confirmed the computer was password protected, and had the built-in capability to reveal its location if the computer was turned on and connected to the internet
  - The provider received no indication that the computer had been turned on, the password security breached, or that the laptop has been connected to the internet
  - Thus, the provider had no reason to believe that individuals' PHI had been viewed, published online, or used inappropriately

51



Police Report

52

Risk Assessment

- In considering the unauthorized person who used the protected health information or to whom the disclosure was made, the facility, upon learning of the theft, immediately notified the police.

53

Risk Assessment

- Though the provider's investigation pointed to the conclusion that the protected information was neither acquired nor viewed, the provider still took measures necessary in situations involving a breach:
  - Breach Notification to the Office of Civil Rights
  - Notification to the affected individuals within that 60-day timeframe

54

Other Actions Taken In Response

- The provider, in order to prevent this occurrence from happening again, took additional steps to secure its computers and the information stored on its computer.
- One such step was to make sure all computer files were encrypted, ensuring files could not be accessed without a secret key.

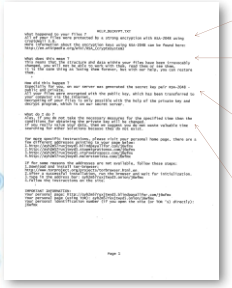
55

HIPAA Breach #2 – Hacking/IT Case Cryptowall Hack

- An email attachment of questionable origin was sent around the organization as part of a multi-pronged attack from an unauthorized user source.
- The source created a ransom requesting discreet communications through links. The business was directed to comply with the demands or force data being destroyed.

56

Ransom Letter



What Happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using cryptowall 3.0

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as loosing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048-public and private. All of your files were encrypted with the public key which has been transferred to your computer via the internet; decrypting of your files is only possible with the help of the private key and decrypt program which is on our secret server

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed. If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

57

The Virus – Ransomware

- The virus at issue was the CryptoWall virus. This virus is typically spread through email as an attachment. Once infected, all files become encrypted; when attempting to open certain files, the files will be launched with the correct program, but will often be jumbled.
- Known as "ransomware," the infection offers the end user a means with which to clean up the infection and recover their files through a decryption key offered in exchange for paying a ransom.

58

The Breach

Under HIPAA, a breach is an impermissible use or disclosure that compromises the security or privacy of the protected health information.

The provider undertook an investigation to evaluate the probability that the CryptoWall virus caused the privacy or security of the protected health information involved to be compromised – to evaluate if a reportable breach occurred.

59

Reportable or Not Reportable?

The provider did a number of things:

- It retained the services of a consultant to analyze the system to determine if PHI was accessed
- It conducted staff interviews to learn more about how the virus infected the system
- It conducted a forensic analysis of the machines to assess the security of the protected health information

While the investigation continues, regardless of the outcome, the facility will be taking action.

60

First Outcome

- If the facility determines that there is a low probability that PHI has been compromised – that the breach is not reportable, the facility still has an opportunity to strengthen HIPAA compliance to ensure as much as possible that another potential breach does not occur.
- A Risk Analysis should be conducted, which is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by that entity or business associate.

61

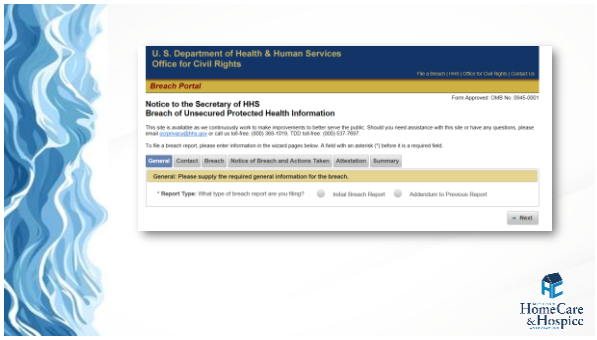
Second Outcome

- If the facility determines that PHI has been compromised – that the breach is reportable, the facility will have to undertake steps for notification.
- It will have to determine the affected number of individuals to ascertain reporting requirements, and in accordance with whichever requirements apply, it will then have to report to the affected individuals, the HHS, and perhaps to the media.
- In addition, it will be necessary to comply with state laws as well, as state agencies may have different reporting requirements.

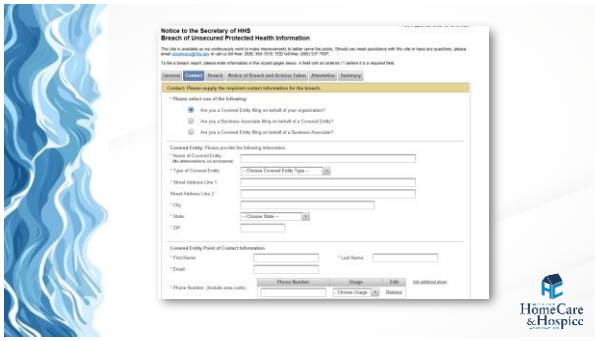
62

HIPAA Breaches: Submitting a Breach Report to the OCR

63


U. S. Department of Health & Human Services
Office for Civil Rights
Breach Portal
Notice to the Secretary of HHS
Breach of Unsecured Protected Health Information
General
Contact
Breach
Notice of Breach and Actions Taken
Attestation
Summary
General: Please supply the required general information for the breach.
* Report Type: What type of breach report are you filing?
Initial Breach Report
Addendum to Previous Report
Next

64

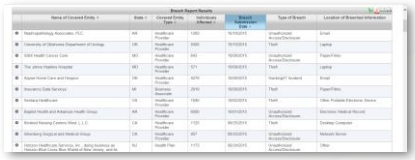

Notice to the Secretary of HHS
Breach of Unsecured Protected Health Information
Contact: Please supply the required contact information for the breach.

65


* Brief Description of the Breach:

66

- As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These 500+ breaches are posted in an accessible format that allows users to search and sort the posted breaches. Additionally, the posted list includes the brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary.

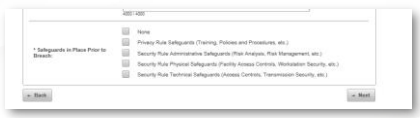


67

Examples of Brief Summaries

- A facility where the covered entity (CE) had stored its medical records since 1994 was sold to a third party and possession of this property was given to the new owner for five days, unbeknownst to the CE. The protected health information (PHI) involved in the breach included the clinical, demographic and financial information of 8,300 individuals. Upon discovery of the breach, the CE immediately retrieved all records at the facility. There was no evidence that the records were otherwise compromised. The CE provided breach notification to HHS, affected individuals, and the media. The CE retrained employees on its revised policies and procedures, including the proper storage of PHI and distribution of its revised policies and procedures. OCR obtained assurances that the CE implemented the corrective actions listed.

68



69

HIPAA Breaches: What Happens After A Report Is Filed

70

The OCR Investigation

- Once an organization has reported a breach to the HHS, the OCR will investigate
- The OCR, may, on its own, after receiving a complaint from a third party, may initiate an investigation prior to the Breach Notification

71

The OCR Investigation - Audits

- Because health information technology poses new risks to consumer privacy, HITECH requires HHS to perform periodic audits of covered entities to ensure compliance with privacy rules.
  - In circumstances where an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited organization that could lead to civil money penalties
- All covered entities and business associates are eligible to be audited
- Initiated through email
- Check SPAM folders (OSOCRAudit@hhs.gov)
- Desk audits and document requests
- Possibility of on-site audits
- Provider responses
- Compliance reviews

72

Potential Ramifications

- **Resolution Agreements**
  - A contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS, generally for a period of three years.
  - During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement likely would include the payment of a resolution amount.
  - These agreements are reserved to settle investigations with more serious outcomes.

73

Potential Ramifications

- **Civil Monetary Penalties**
  - When HHS has not been able to reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means (monetary settlements + compliance programs), civil money penalties (CMPs) may be imposed for noncompliance against a covered entity.

74

QUESTIONS?

75


HIPAA
Compliance
in Home Care
HEIGHTEN YOUR
COMPLIANCE
Michigan HomeCare &
Hospice Association
Michael Kern
Kitch Attorneys & Counselors
One Woodward Avenue, Suite 2400
Detroit, MI 48226-5485
313.965.7586
michael.kern@kitch.com
www.kitch.com
KITCH
Attorneys & Counselors
Detroit Lansing Mt. Clemens
Toledo Chicago
HomeCare
& Hospice

76