

HIPAA: Best Practices to Securing Patient Privacy

CareQuest Institute Continuing Education Webinar

July 11, 2024

Housekeeping

- We will keep all lines muted to avoid background noise.
- We will send a copy of the slides and a link to the recording via email after the live program.
- We'll also make the slides and recording available on carequest.org.

To receive CE Credits:

- Look for the evaluation form, which we'll send via email within 24 hours.
- Complete the evaluation by **Friday, July 19**.
- Eligible participants will receive a certificate soon after via email.

We appreciate your feedback to help us improve future programs!



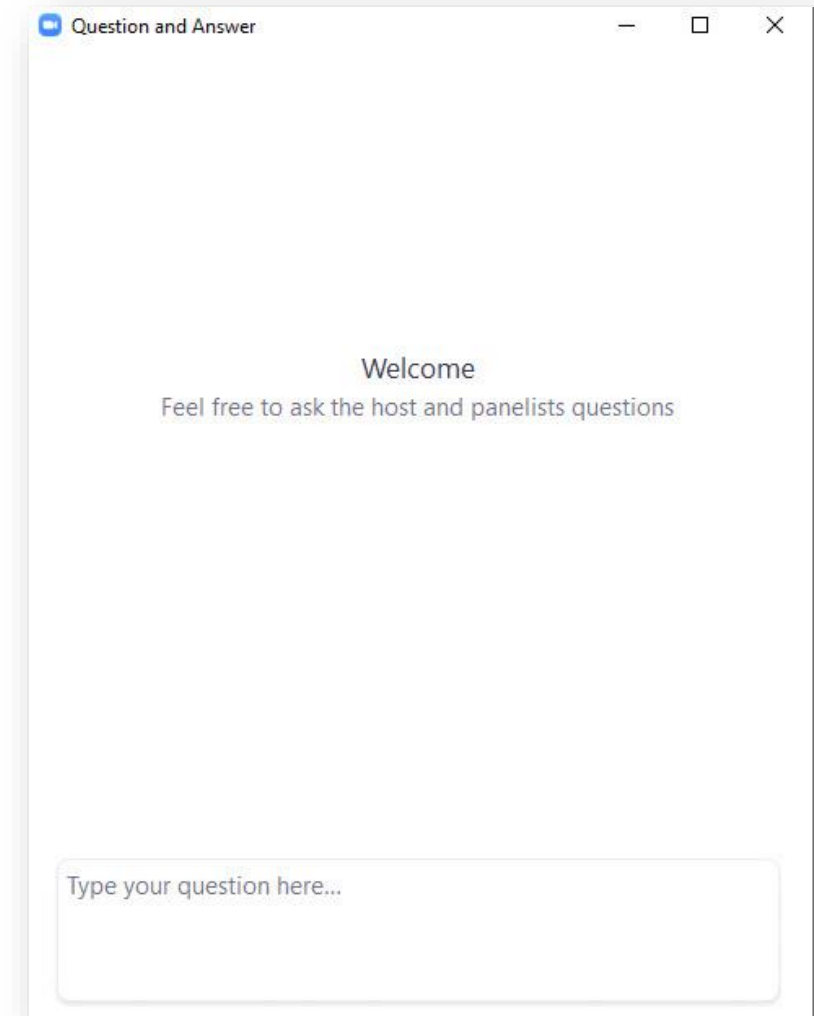
The CareQuest Institute for Oral Health is an ADA CER-P Recognized Provider. This presentation has been planned and implemented in accordance with the standards of the ADA CER-P.

*Full disclosures available upon request



Question & Answer Logistics

- Feel free to enter your questions into the **Question & Answer box** throughout the presentations.
- We will turn to your questions and comments toward the end of the hour.



Learning Objectives

- Identify the fundamental principles of HIPAA, including general privacy rules, security rules, and breach notification rule standards.
- Explain the significance of HIPAA compliance in dental practice, the importance of protecting patient health information (PHI), and potential consequences of non-compliance.
- Apply HIPAA privacy and security rules to everyday scenarios in dental practice, including managing social media disclosures, website tracking technologies, and PHI breaches.

HIPAA: Best Practices to Securing Patient Privacy



WEBINAR | Thursday, July 11, 2024 | 7–8 p.m. ET | ADA CERP Credits: 1

MODERATOR



Hannah Cheung,
MPH, MS, RDH
Health Sciences Specialist,
CareQuest Institute for Oral Health

PRESENTER



Alisa Lewis
Director, Governance Risk and
Compliance, CareQuest Institute
for Oral Health

HIPAA: Best Practices to Securing Patient Privacy

CareQuest Institute Continuing Education Webinar

July 11, 2024

Polling Question

Which is correct?

- a) HIPPA
- b) HIPPO
- c) HIPAA
- d) HIPOO

HIPAA Overview

Health Information Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

Part 164 of the Regulations includes the Privacy Rule, Security Rule, and Breach Notification Rule

Covered Entity vs. Business Associate



A **covered entity** includes health care providers, health plans, and health care clearinghouses who electronically transmit any health information in connection with certain financial and administrative transactions (such as electronically billing health insurance carriers for services), or a health care clearinghouse.

A **business associate** is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. If the business associate uses a subcontractor to carry out such services or functions, then the subcontractor would be the business associate's business associate.

Applicability



PRIVACY RULE APPLIES TO COVERED ENTITIES AND IN PART, TO BUSINESS ASSOCIATES



SECURITY RULE AND THE BREACH NOTIFICATION RULE APPLY TO BOTH COVERED ENTITIES AND BUSINESS ASSOCIATES

Polling Question

Which of the following is NOT considered a business associate?

- a) An attorney whose legal services to a health plan involve access to protected health information
- b) A cleaning service that cleans a provider's office
- c) An independent medical transcriptionist that provides transcription services to a dentist

Why HIPAA Compliance Is Important



Protects patient's health information



Required by federal regulations



Assures your patients you are appropriately safeguarding their data

Risks of HIPAA Compliance Violations

Fines and penalties

Jail time

Negative press

Corrective action plans from OCR

Settlement costs

Loss of patients' and customers' trust

Risks of HIPAA Compliance Violations

Fines and
penalties

ACPM Podiatry HIPAA Enforcement Action

Risks of HIPAA Compliance Violations

Jail time

ACPM Podiatry HIPAA Enforcement Action

Former Hospital Employee Sentenced for HIPAA Violations

Risks of HIPAA Compliance Violations

Negative press

**Hospital draws HIPAA heat after
NFL medical record tweet**

ACPM Podiatry HIPAA Enforcement Action

Former Hospital Employee Sentenced for HIPAA
Violations

Risks of HIPAA Compliance Violations

**Life Hopes Resolution Agreement and Correction
Action Plan**

Hospital draws HIPAA heat after
NFL medical record tweet

Corrective
action plans
from OCR

HIPAA Enforcement Action

Former Hospital Employee Sentenced for HIPAA
Violations

Risks of HIPAA Compliance Violations

Memorial Hermann's Use of Patient Name in Press Release Leads to \$2.4 Million HIPAA Settlement

Life Hopes Resolution Agreement and Correction Action Plan

Hospital draws HIPAA heat after NFL medical record tweet

ACPM Podiatry HIPAA Settlement Action

Settlement costs

Employee Sentenced for HIPAA

Risks of HIPAA Compliance Violations

Memorial Hermann's Use of Patient Name in Press Release Leads to \$2.4 Million HIPAA Settlement

The Devastating Business Impacts of a Cyber Breach

Life Hopes Resolution Agreement and Correction Action Plan

Hospital draws HIPAA heat after NFL medical record tweet

ACPM Podiatry HIPAA Enforcement Action

Former Hospital Employee
Violations

Loss of patients' and customers' trust

Hot Topics

- OCR Risk Analysis Initiative Announced
- Website Tracking Technologies – OCR Bulletin
- Social Media Disclosures

OCR Risk Analysis Initiative Announced

HIPAA Audits to begin in 2024

Be prepared:

- ✓ Security Risk Analysis and Risk Management Plan is up to date – conduct regularly and when new technologies and business operations are planned
- ✓ Incorporate lessons learned from incidents into overall security management process
- ✓ HIPAA policies and procedures in place and finalized
- ✓ Provide training and awareness to workforce members

Website Tracking Technologies – OCR Bulletin

- Website tracking technologies are used to collect and analyze information about how website visitors interact with your websites or mobile applications
- HIPAA Rules apply when PHI is collected through the tracking technologies or PHI is disclosed to tracking technology vendors
- Cannot share PHI with tracking technology vendors unless 1) there is an authorization from the individual **or** 2) disclosure to the tracking technology vendor is permitted under the Privacy Rule **and** there is a business associate agreement in place with the vendor

Website Tracking Technologies – OCR Bulletin

- On June 20, 2024, US District Court of Northern District of Texas vacated a part of the HHS guidance

**Unauthenticated public webpages and IP addresses
 (“Proscribed Combination”)**

Vs

Authenticated webpages and IHI

- HHS is considering next steps, which could include an appeal

Website Tracking Technologies: How to Protect Your Organization


Do you use third party tracking technology on your organization's website? Are you sharing PHI to these third parties?

- ✓ Ensure all disclosures comply with the Privacy Rule and are minimum necessary
- ✓ Establish a BAA with tracking technology vendor
- ✓ Address use of tracking technologies in Risk Analysis and Risk Management processes
- ✓ Provide breach notification to individuals and to HHS Secretary if an unauthorized disclosure occurred



COSMOS
Navigate the Compliance Universe

Compliance Today - April 2024

 Alisa Lewis (alewis@carequest.org, [linkedin.com/in/alisa-lewis-chc-crisc/](https://www.linkedin.com/in/alisa-lewis-chc-crisc/)) is the Governance, Risk, and Compliance Director at CareQuest Institute for Oral Health Inc. in Boston, MA.

Compliance considerations for website tracking technologies

by Alisa Lewis, CHC, CRISC

Many of you may have seen the December 2022 bulletin issued by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) reminding regulated entities they are “not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI [protected health information] to tracking technology vendors or any other violations of the HIPAA Rules.”^[1] In July 2023, the Federal Trade Commission (FTC) and OCR issued a joint warning letter to 130 hospital systems and telehealth providers alerting them to the risks of using website tracking technologies.^[2] The bulletin and warning letters may have prompted you to examine if your websites shared PHI with any third parties and ensure appropriate controls were in place, such as executing business associate agreements. While there is an open lawsuit filed by the American Hospital Association (AHA) and other health systems in November 2023 disputing the rule promulgated by the OCR bulletin because it is “flawed as a matter of law, deficient as a matter of administrative process, and harmful as a matter of policy,” healthcare organizations should not ignore the risks associated with the use of such technology.^[3] Even if the court finds in AHA’s favor, the risk of using tracking technologies is not only associated with a potential HIPAA violation but also the risk of class-action lawsuits and complaints for violating state and other federal laws.

In the past few years, there has been an increase in settlements and litigation against organizations that should prompt you to further examine the use of website tracking technologies and ensure your organization is appropriately mitigating related risks. The cases have involved complaints of both healthcare and nonhealthcare-related entities and have involved a variety of allegations, such as violations of wiretapping and electronic eavesdropping,^[4] the FTC Act,^[5] the Video Privacy Protection Act,^[6] the California Consumer Privacy Act (CCPA)^[7] and other states’ privacy laws, and invasion of privacy under common law. As new consumer privacy laws are passed, the potential for violations could expand. Responding to and defending against such complaints can be costly and have a negative impact on your organization’s reputation.

As a compliance professional, it’s important that you understand what tracking technologies are, potential compliance and legal risks related to the use of tracking technologies, and how to protect your organization against such risks.

Social Media Disclosures

Disclosing PHI on social media without authorization is considered an unauthorized disclosure of information

- ✓ Have a written authorization before sharing PHI on social media
- ✓ Have written policies and procedures prohibiting sharing PHI without written authorization on social media
- ✓ Train personnel on policies and procedures and have them sign acknowledgment of receiving policy

Dental Practice Pays \$10,000 to Settle Social Media Disclosures of Patients' Protected Health Information

\$50,000 Civil Monetary Penalty Imposed on Dental Practice for Social Media HIPAA Violation

What is PHI and ePHI?

Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

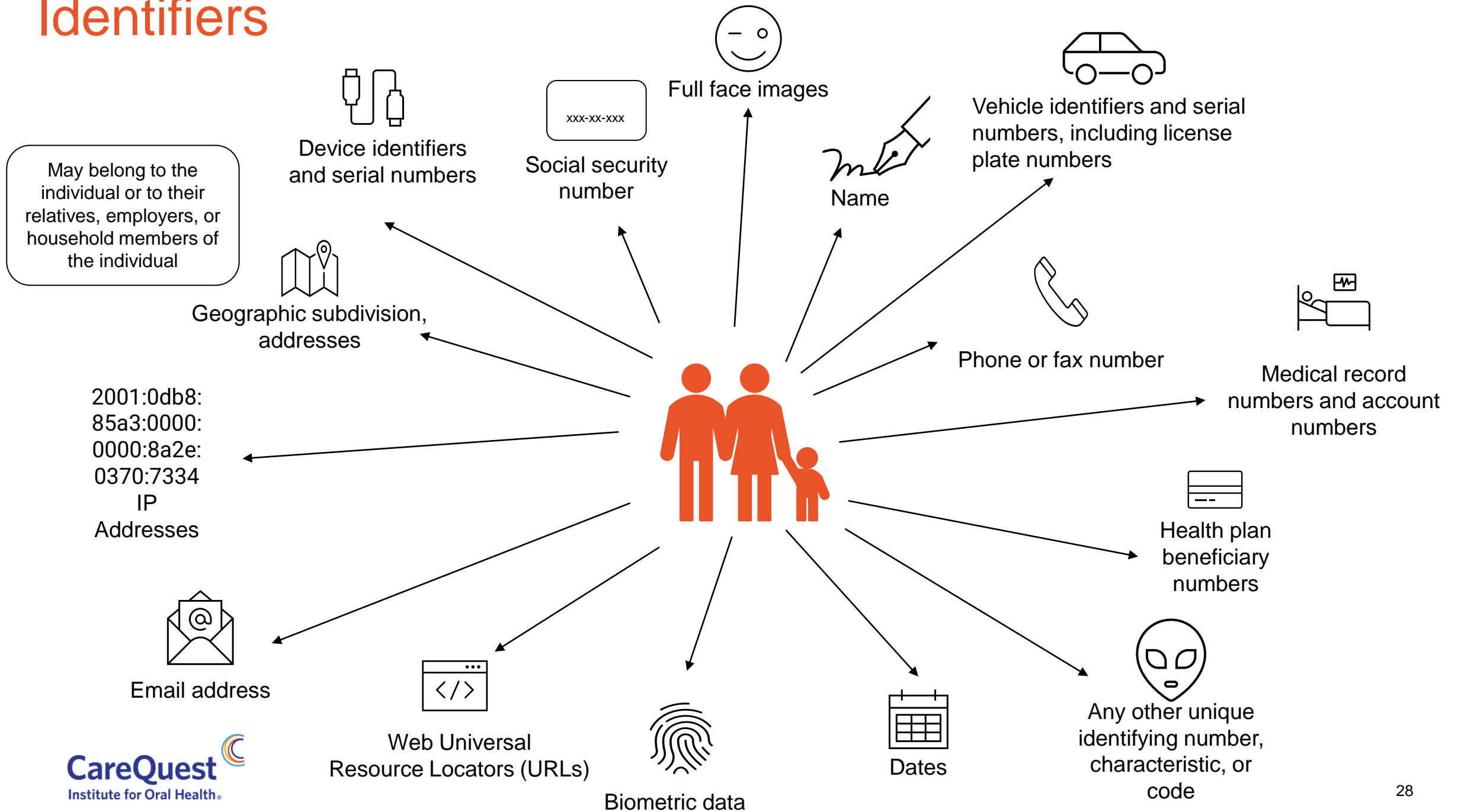
What is PHI?

Individually identifiable health information – information, including demographic data, that relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a *reasonable basis* to believe it can be used to identify the individual.

Identifiers



Any Other Unique Identifying Number, Characteristic, or Code

Identifying Number

“Clinical trial record numbers are included in the general category of ‘any other unique identifying number, characteristic, or code.’ (preamble to the Privacy Rule at 65 FR 82462, 82712 (Dec. 28, 2000))

Identifying Code

A code corresponds to a value that is derived from a non-secure encoding mechanism.

Identifying Characteristic

A *characteristic* may be anything that distinguishes an individual and allows for identification. For example, a unique identifying characteristic could be the occupation of a patient, if it was listed in a record as “current President of State University.”

The Privacy Rule

Goal: to protect individual's health information while allowing the flow of health information to promote high quality care and to protect the public's health and well being

Two main areas addressed in the Rule:

- Uses and disclosures of protected health information
- Patient's rights, such as right of access, right to amend, and the right to a notice of privacy practices



Required PHI Uses and Disclosures: Covered Entity

- To the individual when they request access to or an accounting of their PHI
- To the secretary of HHS to investigate or determine our compliance with HIPAA regulations

Permitted Uses and Disclosures: Covered Entity

Authorization is required to disclose PHI **except** if the disclosure is:

- To the individual, or their personal representative
- For treatment, payment, or health care operations
- Uses and Disclosures with Opportunity to Agree or Object
- Incidental Use and Disclosure
- Public Interest and Benefit Activities
- Limited Data Set

Public Interest and Benefit Activities Include:

- When required by law
- For public health purposes
- To report abuse, neglect, or domestic violence
 - To a health oversight agency
- For judicial and administrative proceedings or law enforcement purposes
 - To a coroner or medical examiner
 - For cadaveric organ, eye, or tissue donation purposes
 - For research purposes
- Avert a serious threat to health or safety
- For specialized government functions
- To comply with workers compensation laws

Minimum Necessary Standard

When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate **must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.**

Identify roles that need access to PHI to carry out specific duties. Reasonable efforts shall be made to limit PHI access based on the roles as identified.

For PHI disclosures made on a routine and recurring basis, must have policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

For PHI disclosures or requests for disclosures that are not routine in nature, must have criteria to limit the request to the information reasonably necessary to accomplish the disclosures or request's purpose.

Patient Rights

HIPAA provides individuals with the following patient rights:

- Access PHI
- Amend PHI
- Receive an accounting of disclosures
- Request restrictions on certain uses and disclosures of PHI
- Confidential communications
- Receive a Notice of Privacy Practices (applicable to covered entities)

Access and amendment of PHI applies to the individual's designated record set.

Recurring HIPAA Compliance Issues: Individual Right of Access

HIPAA Privacy Rule gives individuals a right to timely access to their health records (30 days with a possibility of one 30-day extension), and at a reasonable, cost-based fee

FOR IMMEDIATE RELEASE
September 20, 2022

Contact: HHS Press Office
202-690-6343
media@hhs.gov

OCR Settles Three Cases with Dental Practices for Patient Right of Access under HIPAA

Enforcement Actions Ensure Patients Receive Timely Access to their Records, at a Reasonable Cost

Today, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced the resolution of three investigations concerning potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule's patient right of access provision. These cases are part of a collective effort, bringing the total 41 cases, to drive compliance on right of access under the law.

"These three right of access actions send an important message to dental practices of all sizes that are covered by the HIPAA Rules to ensure they are following the law," said OCR Director Melanie Fontes Rainer. "Patients have a fundamental right under HIPAA to receive their requested medical records, in most cases, within 30 days. I hope that these actions send the message of compliance so that patients do not have to file a complaint with OCR to have their medical records requests fulfilled."

OCR has taken the following enforcement actions that underscore the importance and necessity of compliance with the HIPAA Rules, including the foundational right of access provision:

Recurring HIPAA Compliance Issue: Individual Right of Access

- ✓ Publish and distribute approved written policies and procedures (e.g., Patient's Right Policy, Designated Record Set Policy, Release of Information forms)
- ✓ Have workforce members sign acknowledgment of policy receipt
- ✓ Review policies and procedures at least annually
- ✓ Train your workforce on the procedure
- ✓ Conduct audits to ensure your complying with your procedure
- ✓ Issue sanctions for violations

Polling Question

What are two main areas of the privacy rule?

- a) Uses and disclosures of protected health information
- b) Patient's rights, such as right of access, right to amend, and the right to a notice of privacy practices
- c) Securing ePHI
- d) Notifying individuals of breach

HIPAA Security Rule

Applies to ePHI which is electronic PHI and to Covered Entities and Business Associates

1. Ensure the confidentiality, integrity, and availability of all ePHI
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule
4. Ensure compliance of the Security Rule by its workforce

HIPAA Security Rule

Administrative

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangement

Physical

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Technical

- Access Control
- Integrity
- Person or Entity Authentication
- Transmission Security

Recurring HIPAA Compliance Issue: Security Risk Analysis, Audit Controls, and Information System Activity Review

Montefiore Medical Center

Potential violations identified:

- Accurate and thorough risk analysis
- Implemented procedures to review information system activity
- Implemented hardware, software, or procedural mechanisms to record and examine activity

Result:

\$4,750,000 settlement and Corrective Action Plan (2023)

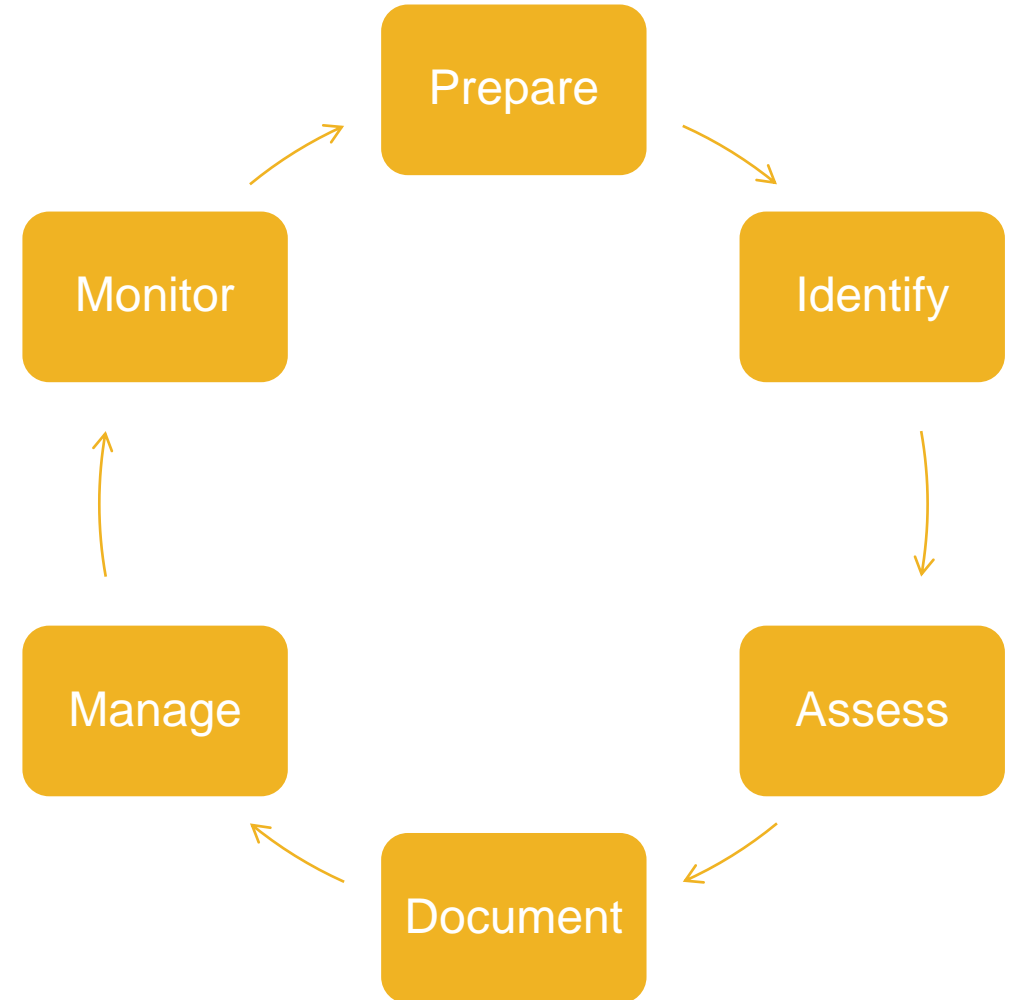


[Primary Care - Montefiore Medical Group - Comprehensive Health Care Center - Primary Care - Specialty Care - Family Medicine - Bronx, New York](#)

Recurring HIPAA Compliance Issue: Security Risk Analysis

Accurate and thorough security risk analysis and risk management is required under the Security Rule

- ✓ Perform periodically or when significant changes to your organization
- ✓ Inventory all facilities, electronic equipment, data systems, programs, and applications that store or maintain ePHI
- ✓ Identify threats and vulnerabilities to the confidential, integrity, and availability of ePHI
- ✓ Include all your facilities and locations, include environmental controls
- ✓ Develop a written risk management plan to address and mitigate risks and vulnerabilities



Recurring HIPAA Compliance Issue: Information System Activity Review and Audit Controls

Information System Activity Review

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

Audit Controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

- ✓ Have documented policies and procedures in place
- ✓ Implement procedures to review activity in ePHI systems, such as audit logs, access reports, and security incident tracking
- ✓ Implement logging mechanisms (hardware, software, procedural mechanisms)
- ✓ Train your workforce members

Recurring HIPAA Compliance Issue: Business Associate Agreements

- Raleigh Orthopaedic Clinic of NC - \$750,000 settlement
- Center for Children's Digestive Health - \$31,000 settlement

You cannot share PHI with a business associate without a BAA in place

BAAs must include certain provisions

Protect your organization:

- Inventory your vendors and identify which provide services or functions involving PHI
- Ensure current BAAs are in place and fully executed

Best Practices

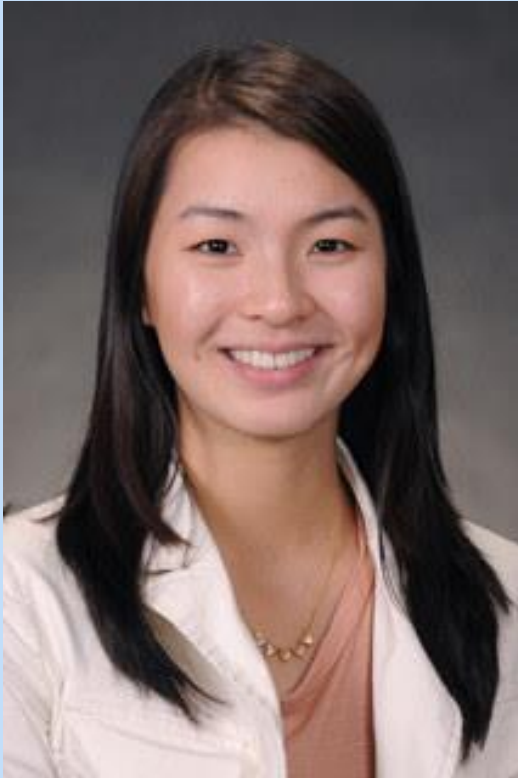
- ✓ Documented **policies and procedures**; review annually
- ✓ **Train workforce members** specific to your organization's policies and procedures and their job roles
- ✓ Perform annual **HIPAA Security Risk Analyses** and continue Risk Management practices
- ✓ Identify all business associates and ensure **business associate agreements** are in place
- ✓ **Monitor and/or audit** to make sure your workforce is adhering to policies and procedures



Alisa Lewis

Director, Governance Risk and Compliance
CareQuest Institute for Oral Health
alewis@carequest.org

Question & Answer



Hannah Cheung, MPH, MS, RDH
Health Sciences Specialist
CareQuest Institute for Oral Health
hcheung@carequest.org

To Explore More Industry-Leading Research

CareQuest
Institute for Oral Health.

Who We Are Latest News Careers [Log in/Register](#)

Reimagining Oral Health How We Work Topics Resources & Tools Education & Training

Resource Library

We publish white papers, research reports, briefs, articles, posters, infographics, and tools on topics ranging from adult dental benefits to teledentistry. Use the filters below to find resources by type or topic.

Search by Keyword **Filter by Topic** **Filter by Type**

Title	Topic	Type
Improving Care Coordination Between Oral and Medical Providers	Care Coordination	Video
Veteran Oral Health: Expanding Access and Equity	Expanding Access	White Paper
2021 Oral Health Information Technology Virtual Convening	Care Coordination	Presentation
Dental Fear Is Real. Providers Can Help.	Expanding Access, Health Equity	Visual Report
Why We (Still) Need to Add Dental to Medicare	Adult Dental Benefit, Expanding Access, Health Equity	Report
A Cross-Sectional Analysis of Oral Health Care Spending over the Life Span in Commercial- and Medicaid-Insured Populations	Expanding Access, Health Equity	Article
Time Is on the Side of Change in Dentistry	COVID-19 and Oral Health, Health	Article

www.carequest.org/resource-library

CareQuest
Institute for Oral Health.

Uninsured and in Need

68.5 Million Lack Dental Insurance, More May Be Coming

State of Oral Health Equity in America 2023

According to the 2023 State of Oral Health Equity in America (SOHEA) survey from CareQuest Institute for Oral Health®, an estimated 68.5 million adults in the US do not have dental insurance.

The estimated portion of the population without dental insurance (27%) is significantly greater than that of those without health insurance (9%) — about three times as high. With a significant number of adults in the US lacking dental insurance, we face an ongoing nationwide oral health crisis. We must call for health care professionals, administrators, policymakers, and advocates to lead efforts to increase dental coverage by Medicaid and Medicare.

SOHEA is the largest nationally representative survey focused exclusively on adults' knowledge, attitudes, experiences, and behaviors related to oral health. The 2023 survey found that of all adult age groups, adults 60 years and older (33%) were most likely to lack dental insurance. Additionally, adults living in rural areas (34%) were more likely to lack dental insurance than adults living in suburban (24%) or urban (29%) areas.

While the proportion of adults with dental insurance increased by 3% from 2021 to 2023, it is important to note that the SOHEA survey did not ask survey participants whether they gained dental coverage in the past year. The increase in dental insurance rates is likely related, at least in part, to the increase in the proportion of adults receiving dental coverage through Medicare Advantage within the past year — from 7% in 2022 to 9% in 2023. During that same time period, Medicare enrollment increased from 65.1 million to 65.8 million individuals. Of those enrolled in Medicare, the proportion selecting Medicare Advantage plans also increased from 46% to 48%. While it is positive that more Medicare-eligible adults are selecting coverage with some dental benefits, it is important to note that the scope of dental benefits under Medicare Advantage plans varies widely and is quite limited, often resulting in high out-of-pocket costs for individuals with severe dental needs. Additionally, Medicare Advantage plans have an estimated average monthly premium of about \$18, and in some cases much higher, again reinforcing the limitations and inaccessibility of this option for Medicare participants seeking oral health coverage.

% of Adults Without Dental Insurance by Age

Age Group	% of Adults Without Dental Insurance
18-29	29%
30-44	19.5%
45-59	24%
60+	33%

Insurance Coverage Trends, 2021-2023

Year	% of adults with dental insurance	% of adults with health insurance
2021	70%	90%
2022	70%	90.1%
2023	73%	90.7%

Webinar Evaluation

Complete the evaluation by **Friday, July 19** to receive CE credit. You will receive a link to the survey within 24 hours.

Next Webinar:

Infection Control: Lessons Learned from the New 'If Saliva Were Red' Video on **July 25 at 7 p.m. ET**

And we invite you to take a minute to sign up for our newsletter to get more information on future webinars!

Sign up for News and Updates

Email*

CareQuest Institute for Oral Health uses the information you provide to share updates on work and offerings to improve the oral health of all. You may unsubscribe at any time (See [Privacy Policy](#)).

Submit



Stay Connected

Follow us on social media



@CareQuestInstitute



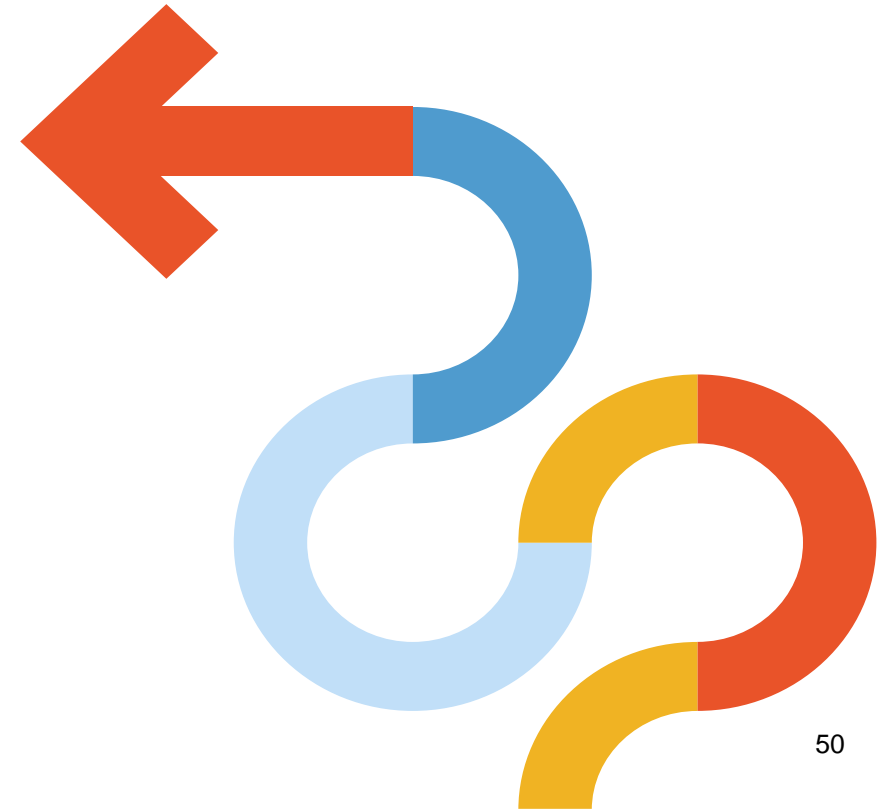
@CareQuestInstitute



@CareQuestInst



CareQuest Institute



CareQuest 
Institute for Oral Health®