December 28, 2023

Nuvance Health has long emphasized the important role that compliance training and education plays in: (i) carrying out organizational-wide compliance initiatives; and (ii) serving as an integral component of its organizational culture of compliance and ethics. As part of our education efforts, we are providing each Nuvance Health workforce member, business affiliate, and agent (collectively "Covered Individuals") with the Centers for Medicare and Medicaid Services ("CMS") Medicare Learning Network *Medicare Parts C and D General Compliance Training Web-Based Training Course* (1/19)("*Medicare Parts C & D Training*"). The Medicare Parts C & D Training is available to Covered Individuals on Nuvance Health's The Hub intranet page and external websites as follows:

- **Nuvance Health East**
  - **The HUB**
  - **External**
- **Nuvance Health West**
  - **The HUB**
  - **External**

Background

Briefly, CMS designed the *Medicare Parts C & D Training* to assist Medicare Advantage Organizations ("MAOs") and their enrolled providers (such as Nuvance Health) in understanding general compliance program requirements. Nuvance Health is providing this information on its own behalf and on behalf of its affiliates Danbury Hospital (which includes its New Milford Hospital campus), Northern Dutchess Hospital, Norwalk Hospital, Putnam Hospital, Sharon Hospital, Vassar Brothers Medical Center, Nuvance Health Medical Practice, P.C., Eastern New York Medical Services, P.C., Nuvance Health Medical Practice CT, Inc., Health Quest Home Care, Western Connecticut Home Care, WCHN Affiliates, Health Quest Affiliates, and the Heart Center.

Why is the Medicare C & D Training Important?

As a Covered Individual, your awareness of the educational materials highlighted in the *Medicare Parts C & D Training* will serve as an important role in ensuring that you carry out your Nuvance Health responsibilities, duties, and functions in a manner that is both legally compliant and in accordance with Nuvance Health's internal standards of conduct. As such, all Covered Individuals are expected to review and become familiar with the content of the *Medicare Parts C & D Training*, which covers, among other important compliance topics, the following: (i) compliance program core elements; and (ii) compliance-related reporting obligations.

What Do I Need To Do?

Please review the Medicare C & D Training in its entirety (which includes the review of all attachments and the completion of the Post-Assessment Test on pages 33-43). If you have any difficulties engaging with this or any other required training in English, please contact the Learning and Talent Development team at learningandtalentdevelopment@nuvancehealth.org to identify alternatives in other languages. ***Note, there are no further actions that you need to take once you have finished reviewing the training***.

Questions Regarding the Medicare C & D Training

Covered Individuals are reminded that they may contact the Corporate Compliance Office, as listed below, to seek guidance or ask questions regarding the *Medicare Parts C & D Training*, or if they have a compliance concern that they wish to report.

- ***General E-mail Address:*** **Compliance@nuvancehealth.org**
- ***Office Line*****:** 203-739-7110
- ***General Facsimile Line:*** 845-475-9761
- **Online web submission: www.nuvancehealth.ethicspoint.com**
- ***24-hour Confidential and Anonymous Compliance Helpline:***

  - **844.YES.WeComply** (for Covered Individuals at Nuvance Health West)
  - **1-844-395-9331** (for Covered Individuals at Nuvance Health East)

Note, Nuvance Health strictly enforces its non-retaliation policies and takes every effort to protect whistleblowers from retribution, intimidation, harassment, and other retaliatory acts. Remember, ***Ask Questions. Voice Your Concerns. Report Improper Conduct***.

As another year comes to an end, we would like to express our sincerest gratitude to all Covered Individuals for their ongoing support of organizational-wide compliance initiatives. The Corporate Compliance Office looks forward to working with each of you to further strengthen the Nuvance Health Compliance and Ethics Program in the upcoming year.

Medicare Parts C and D General Compliance Training
Web-Based Training Course

2023 Nuvance Health Update*

*Except for the "2023 Nuvance Health Update" provided above on this page, the notes outlined on pages 14 & 23, the key points outlined on pages 15-16 & 19, the changes noted on page 33, and the information provided in Appendices "C" to "I", the following document was reproduced from the CMS Medicare Parts C & D General Compliance Training Web-Based Training Course (1/2019) (available at: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/MedCandDGenCompdownload.pdf)

Appendices "D" (available at: https://www.cms.gov/outreach-and-education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf) and "E" (available at: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/se0726factsheet.pdf) are official MLN documents and have not been altered.

Appendices "F" OIG Final Rule: Revisions to the Safe Harbors Under the Anti-Kickback Statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements November 2020 (available at: https://oig.hhs.gov/reports-and-publications/federal-register-notices/factsheet-rule-beneficiary-inducements.pdf), "G" (available at: https://oig.hhs.gov/documents/provider-compliance-training/944/OperatinganEffectiveComplianceProgramFinalBR508.pdf and https://oig.hhs.gov/documents/provider-compliance-training/945/Compliance101tips508.pdf)and "H" (available at: https://oig.hhs.gov/documents/provider-compliance-training/942/ListofComplianceResourcesHandoutBR508r1.pdf) are official U.S. Department of Health and Human Services documents and have not been altered.

Appendix "I" is an internal Nuvance Health document except for Attachment "A" of the same, which is an official guidance document from the Office of the National Coordinator for Health Information Technology and the HHS Office of Civil Rights (available at: https://www.healthit.gov/sites/default/files/YourHealthInformationYourRights_Infographic-Web.pdf). Appendix "J" is an internal Nuvance Health document.

TABLE OF CONTENTS

ACRONYMS

The following acronyms are used throughout the course.

ACRONYM	TITLE TEXT
CFR	Code of Federal Regulations
CMS	Centers for Medicare& Medicaid Services
FDR	First-tier, Downstream, and Related Entity
FWA	Fraud, Waste, and Abuse
HHS	U.S. Department ot Health *Sr* Human Services
MA	Medicare Advantage
MAO	Medicare Advantage Organization
MA-PD	MA Prescription Drug
MLN	Medicare Learning Network®
OIG	Office of Inspector General
PDP	Prescription Drug Plan

TITLE

TITLE PAGE

Click Anywhere or Press Enter to Begin the Web-Based Training Course

INTRODUCTION

INTRODUCTION PAGE 1

The Medicare Parts C and D General Compliance Training course is brought to you by the Medicare Learning Network®

INTRODUCTION PAGE 2

The Medicare Learning Network® (MLN) offers free educational materials for health care professionals on the Centers for Medicare & Medicaid Services (CMS) programs, policies, and initiatives. Get quick access to the information you need.

- **Publications & Multimedia**
- **Events & Training**
- **Newsletters & Social**
- **Continuing Education**

Medicare Learning Network

HYPERLINK URL	TEXT/IMAGE
https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/index.html	Publications & Multimedia
https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNGenInfo/Events-and-Training.html	Events & Training
https://www.cms.gov/Outreach-and-Education/Outreach/FFSProvPartProg/Index.html	Newsletters & Social Media
https://www.cms.gov/Outreach-and-Education/Medicare-Leaming-Network-MLN/MLNGenlnfo /Continuing-Education.html	Continuing Education

INTRODUCTION PAGE3

This training assists Medicare Parts C and D plan Sponsors' employees, governing body members, and their first-tier, downstream, and related entities (FDRs) to satisfy their annual general compliance training requirements in the regulations and sub-regulatory guidance at:

- **42 Code of Federal Regulations (CFR) Section 422.503(b)(4)(vi)(C)**
- **42 CFR Section 423.504(b)(4)(vi)(C)**
- **Section 50.3 of the Compliance Program Guidelines (Chapter 9 of the Medicare Prescription Drug Benefit Manual and Chapter 21 of the Medicare Managed Care Manual)**
- **The "Downloads" section of the CMS Compliance Program Policy and Guidance webpage**

Completing this training in and of itself does not ensure a Sponsor has an "effective Compliance Program." Sponsors and their FDRs are responsible for establishing and executing an effective compliance program according to the CMS regulations and program guidelines.

HYPERLINK URL	TEXT/IMAGE
https://www.ecfr.gov/cgi-bin/text-idx?SID=c66a16ad53319afd0580db00f12c5572&mc=true&node=pt42.3.422&rgn=div5	42 Code of Federal Regulations (CFR) Section 422.503
https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=5cff780d3df38cc4183f2802223859ba&mc=true&r=PART&n=pt42.3.423	42 CFR Section 423.504
https://www.cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra /Downloads/Chapter9.pdf	Chapter 9 of the Medicare Prescription Drug Benefit Manual
https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf	Chapter 21 of the Medicare Managed Care Manual
https://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-and-Audits/ComplianceProgramPolicyandGuidance.html	CMS Compliance Program Policy and Guidance webpage

INTRODUCTION PAGE 4

Why Do I Need Training?

Every year, billions of dollars are improperly spent because of fraud, waste, and abuse (FWA). It affects everyone-including you. This training helps you detect, correct, and prevent FWA. You are part of the solution.

Compliance is everyone's responsibility! As an individual who provides health or administrative services for Medicare enrollees, every action you take potentially affects Medicare enrollees, the Medicare Program, or the Medicare Trust Fund.

INTRODUCTION PAGE 5

Training Requirements: Plan Employees, Governing Body Members, and First-Tier, Downstream, or Related Entity (FDR) Employees

Certain training requirements apply to people involved in Medicare Parts C and D. All employees of Medicare Advantage Organizations (MAOs) and Prescription Drug Plans (PDPs) (collectively referred to in this course as "Sponsors") must receive training about compliance with CMS program rules.

You may need to complete FWA training within 90 days of your initial hire. More information on other Medicare Parts C and D compliance trainings and answers to common questions is available on the CMS website. Please contact your management team for more information.

Learn more about Medicare Part C

Medicare Part C, or Medicare Advantage (MA), is a health insurance option available to Medicare beneficiaries. Private, Medicare-approved insurance companies run MA programs. These companies arrange for, or directly provide, health care services to the beneficiaries who enroll in an MA plan.

MA plans must cover all services Medicare covers with the exception of hospice care. They provide Part A and Part B benefits and may also include prescription drug coverage and other supplemental benefits.

Learn more about Medicare Part D

Medicare Part D, the Prescription Drug Benefit, provides prescription drug coverage to Medicare beneficiaries enrolled in Part A and/or Part B who enroll in a Medicare Prescription Drug Plan (PDP) or an MA Prescription Drug (MA-PD) plan. Medicare-approved insurance and other companies provide prescription drug coverage to individuals living in a plan's service area.

HYPERLINK URL	TEXT/IMAGE
https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Abuse-MLN4649244-Print-Friendly.pdf	Medicare Parts C and D compliance trainings and answers to common questions

INTRODUCTION PAGE 6

Navigating and Completing This Course

Visit the Resources page for disclaimers, a glossary, and frequently asked questions (FAQs). You may find this information useful as you proceed through this course.

Anyone who provides health or administrative services to Medicare enrollees must satisfy general compliance and FWA training requirements. You may use this course to satisfy the general compliance training requirements.

This course consists of one lesson and a Post-Assessment. Successfully completing the course requires completing the lesson and scoring 70 percent or higher on the Post-Assessment. After successfully completing the Post-Assessment, you'll get instructions to print your certificate. If you do not successfully complete the course, you can review the course material and retake the Post-Assessment.

This course uses cues at various times to provide additional information and functionality. For more information on using these cues, adjusting your screen resolution, and suggested browser settings, select **"HELP".**

You do not have to complete this course in one session; however, you must complete the lesson before exiting the course. You can complete the entire course in about 25 minutes. After you successfully complete this course, you receive instructions on how to print your certificate.

INTRODUCTION PAGE 7

Course Objectives

After completing this course, you should correctly:

- Recognize how a compliance program operates
- Recognize how compliance program violations should be reported

Select the "MAIN MENU" button to return to the Main Menu. Then, select "Lesson: Compliance Program Training."

LESSON: COMPLIANCE PROGRAM TRAINING

LESSON PAGE 1

Introduction and Learning Objectives

This lesson outlines effective compliance programs. It should take about 15 minutes to complete.

After completing this lesson, you should correctly:

- Recognize how a compliance program operates
- Recognize how compliance program violations should be reported

LESSON PAGE 2

Compliance Program Requirement

The Centers for Medicare & Medicaid Services (CMS) requires Sponsors to implement and maintain an effective compliance program for its Medicare Parts C and D plans. An effective compliance program must:

- Articulate and demonstrate an organization's commitment to legal and ethical conduct
- Provide guidance on how to handle compliance questions and concerns
- Provide guidance on how to identify and report compliance violations

LESSON PAGE 3

What Is an Effective Compliance Program?

An effective compliance program fosters a culture of compliance within an organization and, at a minimum:

- Prevents, detects, and corrects non-compliance
- Is fully implemented and is tailored to an organization's unique operations and circumstances
- Has adequate resources
- Promotes the organization's Standards of Conduct
- Establishes clear lines of communication for reporting non-compliance

An effective compliance program is essential to prevent, detect, and correct Medicare non-compliance as well as fraud, waste, and abuse (FWA). It must, at a minimum, include the seven core compliance program requirements.

Note:

Additional Information Regarding the Core Elements of a Compliance Program

As described in detail in pages 14-15 of this lesson, CMS requires that seven core elements be met for a compliance program to be deemed effective. It is important to point out that these seven core elements are, in pertinent part, also enumerated in the U.S. Department of Health and Human Services Office of Inspector General's ("OIG") General Compliance Program Guidance (10/23), the 2023 United States Sentencing Commission's Guidelines Manual § 8B2.1 - *Effective Compliance and Ethics Program,* U.S. Department of Justice, Criminal Division Fraud Section, *Evaluation of Corporate Compliance Programs* (3/23)*,* and New York *Compliance /Fraud, Waste, and Abuse Prevention Program* statutory and regulatory requirements ("NY Part 521 regulations"). Nuvance Health also considers the U.S. Department of Justice Office of the Attorney General's guidance regarding the evaluation of compliance programs outlined in section "D" of its September 15, 2022 Memorandum (authored by Deputy Attorney General Lisa Monaco) *on Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group*.

Anti-Retaliation/Whistleblower Protection

Nuvance has established **anti-retaliation/whistleblower protection requirements - -** which have been incorporated into the Nuvance Health Compliance and Ethics Program. Specifically, Nuvance Health is committed to protecting whistleblowers and strictly prohibits retribution, harassment, intimidation or any other form of retaliation against Covered Individuals *(i.e.,* Nuvance Health workforce members, business affiliates, and agents) or other persons or entities ("Protected Persons") that, in good faith, make a compliance report or complaint, engage in protected activities or have otherwise participated in the Nuvance Health Compliance and Ethics Program. Retaliation includes, but is not limited to, the discharge, discipline, suspension, penalization, demotion, change in responsibilities or any other adverse employment action, negative consequence or detrimental change in the terms or conditions of employment, whether formal or informal, as a result of a Protected Person's good faith participation in the Nuvance Health Compliance and Ethics Program. Additional information regarding Nuvance Health's whistleblower protection policies may be found in Appendix "C."

LESSON PAGE 4

Seven Core Compliance Program Requirements

CMS requires an effective compliance program to include seven core requirements.

1. **Written Policies, Procedures, and Standards of Conduct**

   These articulate the Sponsor's commitment to comply with all applicable Federal and State standards and describe compliance expectations according to the Standards of Conduct.

   Key Points: Written policies and procedures must: (i) implement the program; (ii) identify how compliance issues should be reported; and (iii) describe how compliance issues are reviewed and addressed. Nuvance Health has established the following standards of conduct: (i) *WCHN Code of Conduct & Business Ethics; and (ii) Health Quest Code of Conduct and Health Quest Vendor Code of Conduct.* Information regarding these standards of conduct, the *Nuvance Health Compliance and Ethics Program Charter,* and corresponding written policies and procedures are available on Nuvance Health's internal and external websites as set forth in Appendix "C."

2. **Compliance Officer, Compliance Committee, and High-Level Oversight**

   The Sponsor must designate a compliance officer and a compliance committee accountable and responsible for the activities and status of the compliance program, including issues identified, investigated, and resolved by the compliance program.
   The Sponsor's senior management and governing body must be engaged and exercise reasonable oversight of the Sponsor's compliance program.

   Key Points: At Nuvance Health, the Chief Compliance, Audit and Privacy Officer ("CCAPO") is charged with the day-to-day operation of t he Nuvance Health Compliance & Ethics Program. The CCAPO reports administratively to the President and CEO and functionally to the Audit and Compliance Committee of the Nuvance Health Board of Directors. Additionally, Nuvance Health has established an Executive Compliance Committee to, among other important functions, provide advice and counsel to the CAPPO concerning the implementation o f the Nuvance Health Compliance and Ethics Program. The ECC is chaired by the CCAPO.

3. **Effective Training and Education**
   This covers the elements of the compliance plan as well as preventing, detecting, and reporting FWA. Tailor this training and education to the different employees and their responsibilities and job functions.

   Key Points: At Nuvance Health, all Covered Individuals must receive periodic training and education. The training and education must cover compliance issues and expectations, as well as compliance program operation. New workforce members shall receive training and education as part of their orientation.

Seven Core Compliance Program Requirements (continued)

4. Effective Lines of Communication

Make effective lines of communication accessible to all, ensure confidentiality, and provide methods for anonymous and good-faith compliance issues reporting at Sponsor and first-tier, downstream, or related entity (FDR) levels.

Key Points: Nuvance Health is committed to providing confidential open lines of communication to the CCAPO that are accessible by all Covered Individuals to facilitate the reporting of potential compliance issues. Such open lines of communication shall at all times maintain at least one method for the anonymous reporting of potential compliance issues.

5. Well-Publicized Disciplinary Standards

Sponsor must enforce standards through well-publicized disciplinary guidelines.

Key Points: Nuvance Health has established disciplinary policies to encourage the good faith participation in its compliance and ethics program. Covered Individuals who: (i) violate Nuvance Health's standards of conduct and associated policies and procedures, Federal healthcare program requirements or applicable Federal or State law; (ii) fail to report suspected compliance issues; (iii) participate in the program in a non-compliant manner; (iv) encourage, direct, facilitate or permit (either actively or passively) non- compliant conduct; or (v) fail to assist in the resolution of suspected compliance issues by, for example, refusing to cooperate with investigators or preserve information that is potentially relevant to an impending or active compliance investigation, shall be subject to progressive disciplinary action up to and including termination of employment, contract or other affiliation with Nuvance Health.

6. Effective System for Routine Monitoring, Auditing, and Identifying Compliance Risks

Conduct routine monitoring and auditing of Sponsor's and FDR's operations to evaluate compliance with CMS requirements as well as the overall effectiveness of the compliance program.

Key Points: Compliance risks shall be routinely identified and self-evaluated through, among other measures, internal audits and, as ~~appropriate~~, external audits, to identify potential or actual noncompliance. At the minimum, risk areas evaluated shall include billings; payments; credentialing; medical necessity; quality of care; governance; mandatory reporting; contractor, subcontractor, agent and independent contractor oversight; ordered services; and other risk areas that should with due diligence be identified by Nuvance through organizational experience.

NOTE: Sponsors must ensure FDRs performing delegated administrative or health care service functions concerning the Sponsor's Medicare Parts C and D program comply with Medicare Program requirements.

7. Procedures and System for Prompt Response to Compliance Issues

The Sponsor must use effective measures to respond promptly to non-compliance and undertake appropriate corrective action.

Keys Points: All overpayments identified during self-evaluations or through compliance reporting shall be promptly refunded to their respective payors. Policies and procedures shall be implemented to address compliance issues and reduce their recurrence.

LESSONPAGE 6

Compliance Training: Sponsors and Their FDRs

CMS expects all Sponsors will apply their training requirements and "effective lines of communication" to their FDRs. Having "effective lines of communication" means employees of the Sponsor and the Sponsor's FDRs have several avenues to report compliance concerns.

LESSON PAGE 7

Ethics: Do the Right Thing!

As part of the Medicare Program, you must conduct yourself in an ethical and legal manner. It's about doing the right thing!

- Act fairly and honestly
- Adhere to high ethical standards in all you do
- Comply with all applicable laws, regulations, and CMS requirements
- Report suspected violations

LESSON PAGE 8

How Do You Know What Is Expected of You?

Now that you've read the general ethical guidelines on the previous page, how do you know what is expected of you in a specific situation?

Standards of Conduct (or Code of Conduct) state the organization's compliance expectations and their operational principles and values. Organizational Standards of Conduct vary. The organization should tailor the Standards of Conduct content to their individual organization's culture and business operations. Ask management where to locate your organization's Standards of Conduct. Reporting Standards of Conduct violations and suspected non-compliance is **everyone's** responsibility.

An organization's Standards of Conduct and Policies and Procedures should identify this obligation and tell you how to report suspected non-compliance.

Key Points

- Nuvance promotes the highest level of corporate responsibility and is steadfast in its commitment to ethical conduct and compliance with all: (i) applicable Federal and State laws; and (ii) Federal health program and private payor requirements. All Covered Individuals must perform their work functions, duties and role in a manner that facilitates Nuvance Health's commitment to ethical and legal conduct.
- All Covered Individuals are expected to become familiar with the standards of conduct, the *Nuvance Health Compliance and Ethics Program Charter,* and associated policies and procedures set forth in Appendix "C." Covered Individuals are also expected to be familiar with all policies and procedures related to their Nuvance Health role, duties, and functions.
- All Covered Individuals are required to promote, support and contribute in the resolution of potential, suspected, actual or imminent compliance issues, concerns, reports or other compliance matters by assisting in the investigation of compliance matters, which includes, without limitation: (i) promptly reporting compliance questions, issues or concerns; and (ii) fully cooperating with investigators and being completely truthful and forthcoming regarding any information they may have related to a compliance matter.
- All Covered Individuals are required to adhere to HIPAA privacy and security requirements and safeguard patient and workforce member private and confidential information. Covered Individuals must promptly report any actual or potential privacy incident in furtherance of Nuvance Health's efforts to provide, pursuant to applicable law and Nuvance Health's internal policies and procedures, timely breach notification to affected individuals, the media, and regulatory oversight agencies. Attached hereto as Appendices "D" and "E" are the CMS Medicare Learning Network's *HIPAA Basics for Providers: Privacy, Security and Breach Notification Rules,* and *MLN Fact Sheet - Medical Privacy of Protected Health Information,* respectively. Also attached as Appendix "I" is the Nuvance Health *Patient Rights Under HIPAA - Understanding the Nine (9) Key Patient Rights.* All Covered Individuals are expected to become familiar with these important educational documents.
- All Covered Individuals are required to adhere to the federal anti-kickback statute 42 U.S.C. §1320a-7b(b) and the civil monetary penalty (CMP) law provision prohibiting inducements to beneficiaries, set forth in Appendix "F".

  All Covered Individuals shall avoid any activity, act or other form of conduct that may constitute a violation of: (i) the U.S. Foreign Corrupt Practices Act; or (ii) U.S. Export Controls and Sanction Laws. A link to the Resource Guide to the U.S. Foreign Corrupt Practices Act ("FCPA") (2d ed.) published by the U.S. Department of Justice and the Securities and Exchange Commission may be found in Appendix "J". All Covered Individuals are required to become familiar with this guidance.

LESSON PAGE 9

What Is Non-Compliance?

Non-compliance is conduct that does not conform to the law, Federal health care program requirements, or an organization's ethical and business policies. CMS identified the following Medicare Parts C and D high risk areas:

- Agent/broker misrepresentation
- Appeals and grievance review (for example, coverage and organization determinations)
- Beneficiary notices
- Conflicts of interest
- Claims processing
- Credentialing and provider networks
- Documentation and Timeliness requirements
- Ethics
- FDR oversight and monitoring
- Health Insurance Portability and Accountability Act **(HIPAA) (Note: *See* Appendices "D", "E" & "I")**
- Marketing and enrollment
- Pharmacy, formulary, and benefit administration
- Quality of care

For more information, refer to the Compliance Program Guidelines in the Medicare Prescription Drug Benefit Manual and Medicare Managed Care Manual.

Know the Consequences of Non-Compliance

Failure to follow Medicare Program requirements and CMS guidance can lead to serious consequences, including:

- Contract termination
- Criminal penalties
- Exclusion from participating in all Federal health care programs
- Civil monetary penalties

Additionally, your organization must have disciplinary standards for non-compliant behavior. Those who engage in non-compliant behavior may be subject to any of the following:

- Mandatory training or re-training
- Disciplinary action
- Termination

IIYPERLINK URI	
https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/Pub100_18.pdf	Medicare Prescription Drug Benefit Manual
https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS019326	Medicare Managed Care Manual

LESSON PAGE 10

NON-COMPLIANCE AFFECTS EVERYBODY

Without programs to prevent, detect, and correct non-compliance, we all risk:

Harm to beneficiaries, such as:

- Delayed services
- Denial of benefits
- Difficulty in using providers of choice
- Other hurdles to care

Less money for everyone, due to:

- High insurance copayments
- Higher premiums
- Lower benefits for individuals and employers
- Lower Star ratings
- Lower profits

LESSON PAGE 11

How to Report Potential Non-Compliance

Employees of a Sponsor

- Call the Medicare Compliance Officer
- Make a report through your organization's website
- Call the Compliance Hotline

First-Tier, Downstream, or Related Entity (FDR) Employees

- Talk to a Manager or Supervisor
- Call your Ethics/Compliance Help Line
- Report to the Sponsor

Beneficiaries

- Call the Sponsor's Compliance Hotline or Customer Service
- Make a report through the Sponsor's website
- Call 1-800-Medicare

Don't Hesitate to Report Non-Compliance

When you report suspected non-compliance in good faith, the Sponsor can't retaliate against you.

Each Sponsor must offer reporting methods that are:

- Anonymous
- Confidential
- Non-retaliatory

Note: Covered Individuals may confidentially report compliance issues and concerns as follows:

Address:
Nuvance Health Corporate Compliance Office
100 Reserve Road
Danbury, CT 06810

General E-Mail Address:
Compliance@nuvancehealth.org

General Office Line & Facsimile Line:

(203) 739-7110 (phone) (845) 475-9761 (fax)

24 Hour Confidential & Anonymous Compliance Helpline:
1-844-YES.WeComply (for Covered Individuals at Nuvance Health West)
1-844-395-9331 (for Covered Individuals at Nuvance Health East)

Web submission:
www.nuvancehealth.ethicspoint.com

LESSON PAGE 12

What Happens After Non-Compliance Is Detected?

Non-compliance must be investigated immediately and corrected promptly.

Internal monitoring should ensure:

- No recurrence of the same non-compliance
- Ongoing CMS requirements compliance
- Efficient and effective internal controls
- Protected enrollees

LESSON PAGE 13

What Are Internal Monitoring and Audits?

Internal monitoring activities include regular reviews confirming ongoing compliance and taking effective corrective actions.

Internal auditing is a formal review of compliance with a particular set of standards (for example, policies, procedures, laws, and regulations) used as base measures.

LESSON PAGE 14

Lesson Summary

Organizations must create and maintain compliance programs that, at a minimum, meet the seven core requirements. An effective compliance program fosters a culture of compliance.

To help ensure compliance, behave ethically and follow your organization's Standards of Conduct. Watch for common instances of non-compliance, and report suspected non-compliance.

Know the consequences of non-compliance, and help correct any non-compliance with a corrective action plan that includes ongoing monitoring and auditing.

Compliance Is Everyone's Responsibility!

Prevent: Operate within your organization's ethical expectations to prevent non-compliance!

Detect 84 Report: Report detected potential non-compliance!

Correct: Correct non-compliance to protect beneficiaries and save money!

Note:

- Covered Individuals may find additional information regarding an effective Compliance program as published by the OIG, set forth in Appendix "G"
- Covered Individuals may find recommended compliance resources published by the OIG, CMS and other resources, set forth in Appendix "H"

LESSON PAGE 15

Lesson Review

Now that you completed the lesson, let's do a quick knowledge check. The Post-Assessment course score is unaffected by answering the following questions.

LESSON PAGE 16

Knowledge Check

Select the correct answer.

You discover an unattended email address or fax machine in your office receiving beneficiary appeals requests. You suspect no one is processing the appeals. What should you do?

- A. Contact law enforcement
- B. Nothing
- C. Contact your compliance department (via compliance hotline or other mechanism)
- D. Wait to confirm someone is processing the appeals before taking further action
- E. Contact your supervisor

CORRECT ANSWER: C

LESSON PAGE 17

Knowledge Check

Select the correct answer.

A sales agent, employed by the Sponsor's first-tier, downstream, or related entity (FDR), submitted an application for processing and requested two things: 1) to back-date the enrollment date by one month, and 2) to waive all monthly premiums for the beneficiary. What should you do?

- A. Refuse to change the date or waive the premiums but decide not to mention the request to a supervisor or the compliance department
- B. Make the requested changes because the sales agent determines the beneficiary's start date and monthly premiums
- C. Tell the sales agent you will take care of it but then process the application properly (without the requested revisions)-you will not file a report because you don't want the sales agent to retaliate against you
- D. Process the application properly (without the requested revisions)-inform your supervisor and the compliance officer about the sales agent's request
- E. Contact law enforcement and the Centers for Medicare & Medicaid Services (CMS) to report the sales agent's behavior

CORRECT ANSWER: D

LESSON PAGE 18

Knowledge Check

Select the correct answer.

You work for a Sponsor. Last month, while reviewing a Centers for Medicare & Medicaid Services (CMS) monthly report, you identified multiple individuals not enrolled in the plan but for whom the Sponsor is paid. You spoke to your supervisor who said don't worry about it. This month, you identify the same enrollees on the report again. What should you do?

- A. Decide not to worry about it as your supervisor instructed-you notified your supervisor last month and now it's his responsibility
- B. Although you know about the Sponsor's non-retaliation policy, you are still nervous about reporting-to be safe, you submit a report through your compliance department's anonymous tip line to avoid identification
- C. Wait until the next month to see if the same enrollees appear on the report again, figuring it may take a few months for CMS to reconcile its records-if they are, then you will say something to your supervisor again
- D. Contact law enforcement and CMS to report the discrepancy
- E. Ask your supervisor about the discrepancy again

CORRECT ANSWER: B

LESSON PAGE 19

Knowledge Check

Select the correct answer.

You are performing a regular inventory of the controlled substances in the pharmacy. You discover a minor inventory discrepancy. What should you do?

- A. Call local law enforcement
- B. Perform another review
- C. Contact your compliance department (via compliance hotline or other mechanism)
- D. Discuss your concerns with your supervisor
- E. Follow your pharmacy's procedures

CORRECT ANSWER: E

LESSON PAGE 20

You've completed the lesson!

Now that you have learned about compliance programs, it's time to assess your knowledge. Select the "MAIN MENU" button to return to the course Main Menu. Then, select "Post-Assessment" to begin and complete the course.

POST-ASSESSMENT

POST-ASSESSMENT PAGE 1

Post-Assessment

This brief Post-Assessment asks 10 questions and should take about 10 minutes.

Choose an answer for each question by selecting the button next to your answer. You must select an answer before advancing to the next question. You can only move forward in the Post-Assessment, and you can only try each question once. You may change your answer for a question until you select the "SUBMIT ANSWER" button. After you submit your answer, feedback for the question and the "NEXT" button will appear. Select the "NEXT" button to continue. Do not select the "X" button in the right-hand corner of the window as this will cause you to exit the co urse without recording your progress.

You may print your score when you finish the Post-Assessment. After successfully completing the course, you can print a certificate. Successfully completing the course includes finishing all lessons, scoring 70 percent or higher on the Post-Assessment, and completing the course evaluation. Ins tructions on printing your certificate are available after you pass the Post-Assessment.

Select the "NEXT" button to begin the Post-Assessment.

Note: All questions set forth in this section are reproduced from the CMS Medicare Parts C & D General Compliance Training Web-Based Training Course (1/2019) (available at: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/MedCandDGenCompdownload.pdf) except that: (i) Question # 1 is an original Nuvance Health question: (ii) Question # 4 was modified by adding "retaliatory conduct"; (iii) Question # 7 was modified to reflect New York State Compliance Program requirements; and (iv) the corresponding Answer Key on page 43 was modified, where necessary, to reflect the changes in Questions ##1, 4 & 7.

POST-ASSESSMENT PAGE 2

Question 1 of 10

Select the correct answer.

Compliance is everyone's responsibility. All Nuvance Health Covered Individuals must carry out their respective duties, functions, and role in an ethical and legal manner. Remember, ethics is about doing the right thing! Which of the following below are examples of ethical conduct:

I. Acting fairly and honestly

II. Adhering to high ethical standards in all you do

III. Complying with all applicable laws, regulations, and CMS requirements

IV. Reporting suspected violations of the Nuvance Health Compliance and Ethics Program

A. I & III

B. II only

C. I, II & III

D. All of the above

POST-ASSESSMENT PAGE 3

Question 2 of 10

Select the correct answer.

Ways to report a compliance issue include:

- A. Telephone hotlines
- B. Report on the Sponsor's website
- C. In-person reporting to the compliance department/supervisor
- D. All of the above

POST-ASSESSMENT PAGE 4

Question 3 of 10

Select the correct answer.

What is the policy of non-retaliation?

- A. Allows the Sponsor to discipline employees who violate the Code of Conduct
- B. Prohibits management and supervisor from harassing employees for misconduct
- C. Protects employees who, in good faith, report suspected non-compliance
- D. Prevents fights between employees

POST-ASSESSMENT PAGES

Question 4 of 10

Select the correct answer.

These are examples of issues that can be reported to a Compliance Department: suspected fraud, waste, and abuse (FWA); potential health privacy violation, retaliatory conduct, and unethical behavior/employee misconduct.

- A. True
- B. False

POST-ASSESSMENT PAGE 6

Question 5 of 10

Select the correct answer.

Once a corrective action plan begins addressing non-compliance or fraud, waste, and abuse (FWA) committed by a Sponsor's employee or first-tier, downstream, or related entity's (FDR's) employee, ongoing monitoring of the corrective actions is not necessary.

- A. True
- B. False

POST-ASSESSMENT PAGE7

Question 6 of 10

Select the correct answer.

Medicare Parts C and D plan Sponsors are not required to have a compliance program.

- A. True
- B. False

POST-ASSESSMENT PAGE 8

Question 7 of 10

Select the correct answer.

At a minimum, the Nuvance Health Corporate Compliance and Ethics Program must include seven (7) core requirements to be deemed effective .

- ○ A. True
- ○ B. False

POST-ASSESSMENT PAGE 9

Question 8 of 10

Select the correct answer.

Standards of Conduct are the same for every Medicare Parts C and D Sponsor.

- A. True
- B. False

POST-ASSESSMENT PAGE 10

Question 9 of 10

Select the correct answer.

Correcting non-compliance _____

- A. Protects enrollees, avoids recurrence of the same non-compliance, and promotes efficiency
- B. Ensures bonuses for all employees
- C. Both A. and B.

POST-ASSESSMENT PAGE 11
Question 10 of 10

Select the correct answer.
What are some of the consequences for non-compliance, fraudulent, or unethical behavior?

- ○ A. Disciplinary action
- ● B. Termination of employment
- ○ C. Exclusion from participating in all Federal health care programs
- ○ D. All of the above

ANSWER KEY

1. **D**
2. **D**
3. **C**
4. **A**
5. **B**
6. **B**
7. **A**
8. **B**
9. **A**
10. **D**

APPENDIX "A"

APPENDIX A: RESOURCES

RESOURCES PAGE 1 OF 1

Disclaimers

This Web-Based Training (WBT) course was current at the time it was published or uploaded onto the web. Medicare policy changes frequently so links to the source documents have been provided within the course for your reference.

This course was prepared as a service to the public and is not intended to grant rights or impose obligations. This course may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

The Medicare Learning Network® (MLN)

Glossary

For glossary terms, visit the Centers for Medicare & Medicaid Services Glossary.

URL	TEXT/IMAGE
www.cms.gov/apps/glossary	Centers for Medicare & Medicaid Services Glossary

APPENDIX "B"

APPENDIX B: JOB AIDS

Job Aid A: Seven Core Compliance Program Requirements

The Centers for Medicare & Medicaid Services (CMS) requires that an effective compliance program must include seven core requirements:

1. **Written Policies, Procedures, and Standards of Conduct**
   These articulate the Sponsor's commitment to comply with all applicable Federal and State standards and describe compliance expectations according to the Standards of Conduct.
2. **Compliance Officer, Compliance Committee, and High-Level Oversight**
   The Sponsor must designate a compliance officer and a compliance committee to be accountable and responsible for the activities and status of the compliance program, including issues identified, investigated, and resolved by the compliance program.

   The Sponsor's senior management and governing body must be engaged and exercise reasonable oversight of the Sponsor's compliance program.
3. **Effective Training and Education**
   This covers the elements of the compliance plan as well as prevention, detection, and reporting of fraud, waste, and abuse (FWA). This training and education should be tailored to the different responsibilities and job functions of employees.
4. **Effective Lines of Communication**
   Effective lines of communication must be accessible to all, ensure confidentiality, and provide methods for anonymous and good-faith reporting of compliance issues at Sponsor and first-tier, downstream, or related entity (FDR) levels.
5. **Well-Publicized Disciplinary Standards**
   Sponsor must enforce standards through well-publicized disciplinary guidelines.
6. **Effective System for Routine Monitoring, Auditing, and Identifying Compliance Risks**
   Conduct routine monitoring and auditing of Sponsor's and FDR's operations to evaluate compliance with CMS requirements as well as the overall effectiveness of the compliance program.

   NOTE: Sponsors must ensure FDRs performing delegated administrative or health care service functions concerning the Sponsor's Medicare Parts C and D program comply with Medicare Program requirements.
7. **Procedures and System for Prompt Response to Compliance Issues**
   The Sponsor must use effective measures to respond promptly to non-compliance and undertake appropriate corrective action.

Job Aid B: Resources

Compliance Education Materials: Compliance 101

Health Care Fraud Prevention and Enforcement Action Team Provider Compliance Training

Office of Inspector General's (OIG's) Provider Self-Disclosure Protocol

Part C and Part D Compliance and Audits - Overview

Physician Self-Referral

Avoiding Medicare Fraud & Abuse: A Roadmap for Physicians

Safe Harbor Regulations

URL	TEXT/IMAGE
https://oig.hhs.gov/compliance/101	Compliance Education Materials: Compliance 101
https://oig.hhs.gov/compliance/provider-compliance-training	Health Care Fraud Prevention and Enforcement Action Team Provider Compliance Training
https://oig.hhs.gov/compliance/self-disclosure-info/protocol.asp	Office of lnspector General's (OIG's) Provider Self-Disclosure Protocol
https://www.cms.gov/medicare/compliance-and-audits/part-c-and-part-d-compliance-and-audits	Part C and Part D Compliance and Audits - Overview
https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/index	Physician Self-Referral
https://oig.hhs.gov/documents/physicians-resources/947/roadmap_web_version.pdf	Avoiding Medicare Fraud & Abuse: A Roadmap for Physicians
https://oig.hhs.gov/compliance/safe-harbor-regulations/	Safe Harbor Regulations

APPENDIX "C"

Appendix "C"

Nuvance Health has established standards of conduct, as well as associated written policies and procedures, to: (i) implement the Nuvance Health Compliance and Ethics Program; (ii) identify how compliance issues should be reported; and (iii) describe how compliance issues are reviewed and addressed. These standards of conduct and associated policies, procedures, and internal communications include, without limitation the following, and may be found on the Nuvance Health internal and external websites:

WCHN Code of Conduct & Business Ethics (for Covered Individuals at Nuvance Health East):

https://www.nuvancehealth.org/-/media/pdf-files/compliance-pages/communication-regarding-the-deficit-reduction-act-of-2005/wchn-code-of-conduct-and-business-ethics-92718.pdf

Health Quest Systems, Inc. Code of Conduct (for Covered Individuals at Nuvance Health West):

https://www.nuvancehealth.org/-/media/pdf-files/compliance-pages/communication-regarding-the-deficit-reduction-act-of-2005/ny-code-of-conduct.pdf

Health Quest Systems, Inc. Vendor Code of Conduct (for Covered Individuals at Nuvance Health West):

https://www.nuvancehealth.org/-/media/pdf-files/compliance-pages/compliance/ny-vendor-code-of-conduct.pdf

Nuvance Health Compliance and Ethics Program Charter:

https://www.nuvancehealth.org/-/media/pdf-files/compliance-pages/additional-compliance-resources/nuvance-health-compliance-and-ethics-program-charter.pdf

Nuvance Health Whistleblower Protection Policy:

https://www.nuvancehealth.org/-/media/pdf-files/compliance-pages/additional-compliance-resources/whistleblower-protection-policy---2021.pdf

Memorandum Regarding the Deficit Reduction Act of 2005, Nuvance Health East Intranet:

http://thepulse.wchn.priv/Departments/compliance/Compliance%20Public%20Documents/WCHN%20DRA%20memorandm.pdf

Memorandum Regarding the Deficit Reduction Act of 2005, Nuvance Health West Intranet:

https://dimensions.health-quest.org/sites/auditing/SitePages/Communication%20Regarding%20the%20Deficit%20Reduction%20Act%20of%202005.aspx

APPENDIX “D”

HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules

What's Changed?

- Added Information – Privacy Rule protections and rights, page 3
- Added Information – Keeping PHI private and confidential, page 4
- Added Information – Sharing information with other health care professionals, page 4
- Added Information – Sharing patient information with family members and others, page 4
- Added Information – Incidental disclosures, page 5
- Added Information – Protecting and securing health information when using a mobile device, page 5

You'll find substantive content updates in dark red font.

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
Medicare Learning Network®

Table of Contents

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and gives individuals rights to their health information. HIPAA establishes standards to protect PHI held by these entities and their business associates:

- Health plans
- Health care clearinghouses
- Health care providers that conduct certain health care transactions electronically

When you see "you" in this booklet, we're referring to these covered entities and persons.

This booklet discusses:

- The **Privacy Rule**, which sets national standards for the use and disclosure of protected health information (PHI)
- The **Security Rule**, which specifies safeguards that covered entities and their business associates must use to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)
- The **Breach Notification Rule**, which requires covered entities to notify affected individuals, HHS, and, in some cases, the media of a breach of unsecured PHI

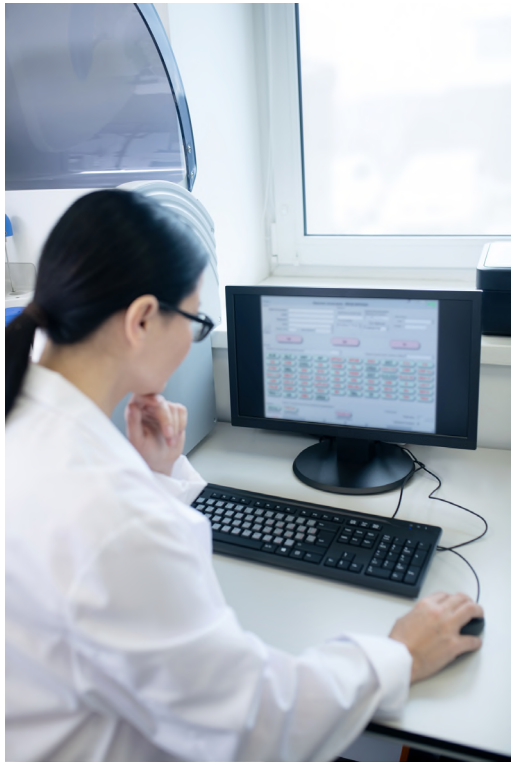
HIPAA Privacy Rule

The Privacy Rule protects your patients' PHI while letting you exchange information to coordinate your patient's care. The Privacy Rule also gives patients the right to examine and get a copy of their medical records, including an electronic copy of their electronic medical records, and to request corrections. Under the Privacy Rule, patients can restrict their health plan's access to information about treatments they paid for in cash, and most health plans can't use or disclose genetic information for underwriting purposes. The Privacy Rule allows you to report child abuse or neglect to the authorities.

PHI

The Privacy Rule protects PHI held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes information about:

- Common identifiers, such as name, address, birth date, and Social Security number
- The 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



Keeping PHI Private & Confidential

The Privacy Rule requires you to:

- Notify patients about their privacy rights and how you use their information
- Adopt privacy procedures and train employees to follow them
- Assign an individual to make sure you're adopting and following privacy procedures
- Secure patient records containing PHI so they aren't readily available to those who don't need to see them

Sharing Information with Other Health Care Professionals

To coordinate your patient's care with other providers, the Privacy Rule lets you:

- Share information with doctors, hospitals, and ambulances for treatment, payment, and health care operations, even without a signed consent form from the patient
- Share information about an incapacitated patient if you believe it's in your patient's best interest
- Use health information for research purposes
- Use email, telephone, or fax machines to communicate with other health care professionals and with patients, as long as you use safeguards

Sharing Patient Information with Family Members & Others

Unless a patient objects, the Privacy Rule lets you:

- Give information to a patient's family, friends, or anyone else identified by the patient as involved in their care

- Give information about the patient's general condition or location to a patient's family member or anyone responsible for the patient's care
- Include basic information in a hospital directory, such as the patient's phone and room number
- Give information about a patient's religious affiliation to members of the clergy

Incidental Disclosures

The HIPAA Privacy Rule requires you to have policies that protect and limit how you use and disclose PHI, but you aren't expected to guarantee the privacy of PHI against all risks. Sometimes, you can't reasonably prevent limited disclosures, even when you're following HIPAA requirements. For example, a hospital visitor may overhear a doctor's confidential conversation with a nurse or glimpse a patient's information on a sign-in sheet. These incidental disclosures aren't considered a HIPAA violation as long as you're following the required reasonable safeguards.

The Office for Civil Rights (OCR) offers guidance about how this applies to health care practices, including an Incidental Uses and Disclosures subcategory in its FAQs.

Securing Health Information When Using a Mobile Device

- Use a password or other user authentication
- Install and enable encryption
- Install and activate remote wiping or remote disabling
- Disable and don't install or use file sharing applications
- Install and enable a firewall
- Install and enable security software
- Keep your security software up to date
- Research mobile applications (apps) before downloading
- Maintain physical control
- Use adequate security to send or receive health information over public Wi-Fi networks
- Delete all stored health information before discarding or reusing the mobile device

Visit the HHS HIPAA Guidance Materials webpage for information about:

- De-identifying PHI to meet HIPAA Privacy Rule requirements
- Individuals' right to access health information
- Permitted uses and disclosures of PHI

HIPAA Security Rule

The HIPAA Security Rule includes security requirements to protect patients' ePHI confidentiality, integrity, and availability. The Security Rule requires you to develop reasonable and appropriate security policies. In addition, you must analyze security risks in your environment and create appropriate solutions. What's reasonable and appropriate depends on your business as well as its size, complexity, and resources. You should always review and modify security measures to continue protecting ePHI in a changing environment.

Specifically, you must:

- Ensure the confidentiality, integrity, and availability of all ePHI you create, receive, maintain, or transmit
- Identify and protect against threats to ePHI security or integrity
- Protect against impermissible uses or disclosures
- Ensure employee compliance

When developing compliant safety measures, consider:

- Size, complexity, and capabilities
- Technical, hardware, and software infrastructure
- The costs of security measures
- The likelihood and possible impact of risks to ePHI

Confidentiality: ePHI can't be available or disclosed to unauthorized persons or processes

Integrity: ePHI can't be altered or destroyed in an unauthorized manner

Availability: ePHI has to be accessible and usable on demand by authorized persons

Visit the HHS HIPAA Guidance Materials webpage for guidance on:

- Administrative, physical, and technical PHI safety measures
- Cybersecurity
- Remote and mobile use of ePHI

HIPAA Breach Notification Rule

When you experience a PHI breach, the HIPAA Breach Notification Rule requires you to notify affected individuals, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The unpermitted use or disclosure of PHI is a breach unless there is a low probability the PHI has been compromised, based on a risk assessment of:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or received the disclosed PHI
- Whether an individual acquired or viewed the PHI
- The extent to which you reduced the PHI risk

You must notify authorities of most breaches without reasonable delay and no later than 60 days after discovering the breach. Submit notifications of smaller breaches affecting fewer than 500 individuals to HHS annually. The Breach Notification Rule also requires business associates to notify a covered entity of breaches at or by the business associate.

Visit the HHS HIPAA Breach Notification Rule webpage for guidance on:

- Administrative requirements and burden of proof
- How to make unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals
- Reporting requirements

Who Must Comply with HIPAA Rules?

Covered entities and business associates must follow HIPAA rules. If you don't meet the definition of a covered entity or business associate, you don't have to comply with the HIPAA rules.

For definitions of covered entity and business associate, see the Code of Federal Regulations (CFR) Title 45, Section 160.103.

Covered Entities

Covered entities that must follow HIPAA standards and requirements include:

- **Covered Health Care Provider:** Any provider of medical or other health care services or supplies that transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard, such as:
  - Doctors
  - Clinics
  - Psychologists
  - Dentists
  - Chiropractors
  - Nursing Homes
  - Pharmacies
- **Health Plan:** Any individual or group plan that provides or pays the cost of health care, such as:
  - Health insurance companies
  - Health maintenance organizations
  - Company health plans
  - Government programs that pay for health care
- **Health Care Clearinghouse:** A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice versa, such as:
  - Billing services
  - Community health management information systems
  - Repricing companies
  - Value-added networks

Business Associates

A business associate is a person or organization, other than a workforce member of a covered entity, that performs functions on behalf of or provides services to a covered entity that involve PHI access. Business associates also include subcontractors responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate.

Business associates provide services to covered entities that include:

- Accreditation
- Billing
- Claims processing
- Consulting
- Data analysis
- Financial services
- Legal services
- Management administration
- Utilization review

Note: A covered entity can be a business associate of another covered entity.

If you work with a business associate, a written contract or other arrangement between you must:

- Detail PHI uses and disclosures the business associate may make
- Require the business associate protect PHI

Visit the HHS HIPAA Covered Entities and Business Associates webpage for more information.

Enforcement

The HHS Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules.

Violations may result in civil monetary penalties. In some cases, U.S. Department of Justice enforced criminal penalties may apply. Common violations include:

- Unpermitted PHI use and disclosure
- Use or disclosure of more than the minimum necessary PHI
- Lack of PHI safeguards
- Lack of administrative, technical, or physical ePHI safeguards
- Lack of individuals' access to their PHI

The following are actual case examples:

- **HIPAA Privacy and Security Rule:** A wireless health service provider agreed to pay $2.5 million to settle potential violations of the HIPAA Privacy and Security Rules after someone stole a laptop with 1,391 individuals' ePHI from an employee's vehicle. The investigation revealed insufficient risk analysis and management processes at the time of the theft. Additionally, the organization's HIPAA Security Rule policies and procedures were in draft form. The organization couldn't produce any final policies or procedures regarding safeguards for ePHI, including for mobile devices.
- **HIPAA Breach Notification Rule:** A specialty clinic agreed to pay $150,000 to settle potential violations of the HIPAA rules. An unencrypted thumb drive with the ePHI of about 2,200 individuals was stolen from a clinic employee's vehicle. The investigation revealed the clinic hadn't accurately or thoroughly analyzed the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. The clinic also didn't comply with Breach Notification Rule requirements for written policies and procedures and employee training. This case was the first settlement with a covered entity for not having policies and procedures to address the HIPAA Breach Notification Rule.

- **Criminal prosecution:** A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining PHI intending to use it for personal gain. He was sentenced to 18 months in federal prison.

Find more information on the HHS HIPAA Enforcement webpage.

Resources

- Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care and Model Notices of Privacy Practices
- FAQs about the Disposal of Protected Health Information
- Business Associate Contracts and Business Associates FAQs
- Fast Facts for Covered Entities and Covered Entity Guidance
- HIPAA FAQs for Professionals
- Omnibus HIPAA Final Rule (2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules)
- Privacy, Security, and HIPAA
- Security Rule Guidance Material
- Training Materials
- Special Topics in Health Information Privacy

APPENDIX “E”

mln FACT SHEET

KNOWLEDGE • RESOURCES • TRAINING

PRINT-FRIENDLY VERSION

MEDICAL PRIVACY OF PROTECTED HEALTH INFORMATION

TARGET AUDIENCE

Medicare Fee-For-Service Providers

The Hyperlink Table at the end of the document provides the complete URL for each hyperlink.

MEDICAL PRIVACY

The Department of Health & Human Services (HHS) Office for Civil Rights (OCR) provides guidance to professionals for the most common Health Insurance Portability and Accountability Act (HIPAA) issues and topics related to medical privacy. Visit the OCR website at https://www.hhs.gov/hipaa/for-professionals/index.html.

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES

Medicare Learning Network®

HEALTH CARE PROFESSIONALS' PRIVACY GUIDE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a Federal law that sets national standards of how health plans, health care clearinghouses, and most health care providers protect the privacy of a patient's health information. Below, find the latest provisions that strengthen the privacy and security protections for health information established under HIPAA.

HEALTH PRIVACY AND SECURITY PROTECTIONS

Some of HIPAA's privacy and security protections for health information include the following:

- Patients may ask for an electronic copy of their electronic medical records
- Patients, paying cash for their treatment, may restrict their health plan's access to that treatment information
- Individuals may authorize their health information for research purposes
- The HIPAA Privacy Rule protects an individual's genetic information and prohibits most health plans from using or disclosing genetic information for underwriting purposes

HIPAA BALANCES PRIVACY AND PATIENT CARE

HIPAA balances patient care and other important purposes while providing Federal protections for individually identifiable information. It does not interfere with the delivery or coordination of health care.

CONSENT FORMS

HIPAA **does not** require patients to sign consent forms before doctors, hospitals, or ambulances may share information for treatment, payment, and health care operations. You may share patient treatment information with other health care professionals without obtaining a signed patient authorization.

INCIDENTAL DISCLOSURES

The Privacy Rule recognizes that it is not practicable to eliminate all risk of incidental disclosures. Incidental disclosures do not violate the rules when you have policies that reasonably safeguard and appropriately limit how protected health information is used and disclosed.

The Office for Civil Rights (OCR) provides guidance about how this applies to customary health care practices (for example, using patient sign-in sheets or nursing station whiteboards, or placing patient charts outside exam rooms).

Search for terms such as "safeguards" or "disclosures" on the Frequently Asked Questions (FAQs) webpage or refer to the Incidental Uses and Disclosures FAQs subcategory.

ELECTRONIC COMMUNICATIONS

HIPAA allows you to use email, the telephone, or fax machines to communicate with patients and other health care professionals using appropriate safeguards to protect patient privacy. Review additional information at https://www.hhs.gov/hipaa/for-professionals/faq/482/does-hipaa-permit-a-doctor-to-share-patient-information-for-treatment-over-the-phone/index.html.

HIPAA Privacy Rule guidance documents related to the electronic exchange of health information are included in the Privacy & Security Resources & Tools webpage.

How Can You Protect and Secure Health Information When Using a Mobile Device?

1. Use a password or other user authentication
2. Install and enable encryption
3. Install and activate remote wiping and/or remote disabling
4. Disable and do not install or use file sharing applications
5. Install and enable a firewall
6. Install and enable security software
7. Keep your security software up to date
8. Research mobile applications (apps) before downloading
9. Maintain physical control
10. Use adequate security to send or receive health information over public Wi-Fi networks
11. Delete all stored health information before discarding or reusing the mobile device

SHARING PATIENT HEALTH STATUS AND LOCATION

Unless a patient objects, HIPAA permits:

- Health care professionals covered by HIPAA may provide information to a patient's family, friends, or anyone else identified by the patient as involved in his or her care
- Hospitals and health care professionals may notify a family member or anyone responsible for the patient's care about the patient's location or general condition
- Hospitals may include basic information such as the patient's phone and room numbers in a hospital directory

For more information, review the Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care guide. Also refer to the Facility Directories FAQs webpage.

MENTAL HEALTH GUIDANCE

For guidance on sharing information related to mental health, visit https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html.

CLERGY AND FAMILY GUIDANCE

Members of the clergy may access a patient's religious affiliation (if provided) and do not have to ask for a patient by name.

If your patient is incapacitated, you may share appropriate information with the patient's family or friends if you believe doing so is in your patient's best interest.

HIPAA does not prevent calls or visits to hospitals by a patient's family or friends, the clergy, or anyone else.

HIPAA DOES NOT PREVENT CHILD ABUSE REPORTING

You may report child abuse or neglect to appropriate government authorities. For more information, search using the term "child abuse" on the FAQs webpage or review the Public Health fact sheet.

For more general information about HIPAA, review:

- Answers to FAQs about HIPAA
- The Uses and Disclosures for Treatment, Payment, and Health Care Operations fact sheet
- The Summary of the HIPAA Privacy Rule
- HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules

Also, the following are examples of some of the most-discussed HIPAA-related FAQ topics on the HHS website:

- Smaller Providers and Businesses
- Right to Access and Research
- Business Associates
- Health Information Technology
- Mental Health

RESOURCES

FOR MORE INFORMATION ABOUT...	RESOURCE
Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care	https://www.hhs.gov/sites/default/files/provider_ffg.pdf
Health Information Privacy	https://www.hhs.gov/hipaa/index.html
Health Information Technology	https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html
Health Insurance Portability and Accountability Act of 1996	https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules	https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/MLN-Publications-Items/ICN909001.html
HIPAA Electronic Communication	https://www.hhs.gov/hipaa/for-professionals/faq/482/does-hipaa-permit-a-doctor-to-share-patient-information-for-treatment-over-the-phone/index.html
HIPAA FAQs for Professionals	https://www.hhs.gov/hipaa/for-professionals/faq
HIPAA FAQs for Professionals - Business Associates	https://www.hhs.gov/hipaa/for-professionals/faq/business-associates
HIPAA FAQs for Professionals - Facility Directories	https://www.hhs.gov/hipaa/for-professionals/faq/facility-directories/index.html
HIPAA FAQs for Professionals - Health Information Technology	https://www.hhs.gov/hipaa/for-professionals/faq/health-information-technology
HIPAA FAQs for Professionals - Incidental Uses and Disclosures	https://www.hhs.gov/hipaa/for-professionals/faq/incidental-uses-and-disclosures/index.html
HIPAA FAQs for Professionals - Mental Health	https://www.hhs.gov/hipaa/for-professionals/faq/mental-health/index.html
HIPAA FAQs for Professionals - Right to Access and Research	https://www.hhs.gov/hipaa/for-professionals/faq/right-to-access-and-research/index.html
HIPAA FAQs for Professionals - Smaller Providers and Businesses	https://www.hhs.gov/hipaa/for-professionals/faq/smaller-providers-and-businesses
HIPAA for Professionals	https://www.hhs.gov/hipaa/for-professionals/index.html
HIPAA's Privacy and Security Protections	https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
HIPAA Privacy Rule and Sharing Information Related to Mental Health	https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html
Information Related to Mental and Behavioral Health, including Opioid Overdose	https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html

FOR MORE INFORMATION ABOUT...	RESOURCE
Incidental Uses and Disclosures	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html
Privacy & Security Resources & Tools	https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-resources-tools
Public Health	https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html
Summary of the HIPAA Privacy Rule	https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
Uses and Disclosures for Treatment, Payment, and Health Care Operations	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html

HYPERLINKS

EMBEDDED HYPERLINK	WEB ADDRESS
Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care	https://www.hhs.gov/sites/default/files/provider_ffg.pdf
Health Information Privacy	https://www.hhs.gov/hipaa/index.html
Health Information Technology	https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html
Health Insurance Portability and Accountability Act of 1996	https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules	https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/MLN-Publications-Items/ICN909001.html
HIPAA Electronic Communication	https://www.hhs.gov/hipaa/for-professionals/faq/482/does-hipaa-permit-a-doctor-to-share-patient-information-for-treatment-over-the-phone/index.html
HIPAA FAQs for Professionals	https://www.hhs.gov/hipaa/for-professionals/faq
HIPAA FAQs for Professionals - Business Associates	https://www.hhs.gov/hipaa/for-professionals/faq/business-associates
HIPAA FAQs for Professionals - Facility Directories	https://www.hhs.gov/hipaa/for-professionals/faq/facility-directories/index.html
HIPAA FAQs for Professionals - Health Information Technology	https://www.hhs.gov/hipaa/for-professionals/faq/health-information-technology
HIPAA FAQs for Professionals - Incidental Uses and Disclosures	https://www.hhs.gov/hipaa/for-professionals/faq/incidental-uses-and-disclosures/index.html

EMBEDDED HYPERLINK	WEB ADDRESS
HIPAA FAQs for Professionals - Mental Health	https://www.hhs.gov/hipaa/for-professionals/faq/mental-health/index.html
HIPAA FAQs for Professionals - Right to Access and Research	https://www.hhs.gov/hipaa/for-professionals/faq/right-to-access-and-research/index.html
HIPAA FAQs for Professionals - Smaller Providers and Businesses	https://www.hhs.gov/hipaa/for-professionals/faq/smaller-providers-and-businesses
HIPAA for Professionals	https://www.hhs.gov/hipaa/for-professionals/index.html
HIPAA's Privacy and Security Protections	https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
HIPAA Privacy Rule and Sharing Information Related to Mental Health	https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html
Information Related to Mental and Behavioral Health, including Opioid Overdose	https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html
Incidental Uses and Disclosures	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html
Privacy & Security Resources & Tools	https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-resources-tools
Public Health	https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html
Summary of the HIPAA Privacy Rule	https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
Uses and Disclosures for Treatment, Payment, and Health Care Operations	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html

Medicare Learning Network® Product Disclaimer

Paid for by the Department of Health & Human Services.

APPENDIX “F”

HHS Office of Inspector General Fact Sheet

Final Rule: Revisions to the Safe Harbors Under the Anti-Kickback Statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements
November 2020

Background

The Office of Inspector General (OIG) of the Department of Health and Human Services (HHS) is publishing a final rule (Final Rule), "Revisions to the Safe Harbors Under the Anti-Kickback Statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements." This Final Rule is part of HHS's Regulatory Sprint to Coordinated Care (Regulatory Sprint), which aims to reduce regulatory barriers to care coordination and accelerate the transformation of the health care system into one that better pays for value and promotes care coordination.

HHS has identified the broad reach of the Federal anti-kickback statute, 42 U.S.C. § 1320a-7b(b), and the civil monetary penalty (CMP) law provision prohibiting inducements to beneficiaries (Beneficiary Inducements CMP), 42 U.S.C. § 1320a-7a(a)(5), as potentially inhibiting beneficial arrangements that would advance the transition to value-based care and improve the coordination of patient care across care settings in both the Federal health care programs and commercial sector.

The Federal anti-kickback statute provides for criminal penalties for whoever knowingly and willfully offers, pays, solicits, or receives remuneration to induce or reward, among other things, the referral of business reimbursable under any of the Federal health care programs, including Medicare and Medicaid. Health care providers and others may voluntarily seek to comply with statutory and regulatory safe harbors so that they have the assurance that their business practices will not be subject to sanctions under the anti-kickback statute. To receive safe harbor protection, an arrangement must squarely meet each requirement of an applicable safe harbor. However, failure to fit in a safe harbor does not mean that an arrangement violates the Federal anti-kickback statute. Arrangements that do not fit in a safe harbor are analyzed on a case-by-case basis, including whether the parties had the requisite intent. Congress intended the safe harbor regulations to be updated periodically to reflect changing business practices and technologies in the health care industry.

The Beneficiary Inducements CMP provides for the imposition of CMPs against any person who offers or transfers remuneration to a Medicare or State health care program beneficiary that the person knows or should know is likely to influence the beneficiary's selection of a particular provider, practitioner, or supplier for the order or receipt of any item or service for which payment may be made, in whole or in part, by Medicare or a State health care program.

OIG promulgated a Notice of Proposed Rulemaking (NPRM) on October 17, 2019.[1] OIG coordinated with the Centers for Medicare & Medicaid Services (CMS), which also issued an NPRM in October 2019, and is concurrently issuing a final rule in connection with the Regulatory Sprint. In response to OIG's NPRM, we received 337 public comments, which

[1] *See* 84 Fed. Reg. 55,694 (Oct. 17, 2019), *available at* https://www.federalregister.gov/documents/2019/10/17/2019-22027/medicare-and-state-healthcare-programs-fraud-and-abuse-revisions-to-safe-harbors-under-the; *see also* OIG, HHS Office of Inspector General Fact Sheet, Notice of Proposed Rulemaking OIG-0936-AA10-p (Oct. 2019), *available at* https://oig.hhs.gov/authorities/docs/2019/CoordinatedCare_FactSheet_October2019.pdf.

provided information regarding whether the proposals in the NPRM would effectively remove barriers to coordinated and value-based care and include the appropriate safeguards to protect Federal health care programs and patients.

The Final Rule

The Final Rule implements seven new safe harbors, modifies four existing safe harbors, and codifies one new exception under the Beneficiary Inducements CMP. The Final Rule modifies and clarifies the NPRM in response to comments and as explained in the preamble to the Final Rule. For example, the Final Rule clarifies how medical device manufacturers and durable medical equipment companies may participate in protected care coordination arrangements that involve digital health technology; lowers the level of "downside" financial risk parties must assume to qualify under the new safe harbor for value-based arrangements with substantial downside financial risk; and, in recognition of the urgent problem of cyber threats to the health care industry, broadens the new safe harbor for cybersecurity technology and services to cover remuneration in the form of cybersecurity-related hardware.

To safeguard against inappropriate incentives, the Final Rule incorporates additional limitations on parties seeking safe harbor protection under the patient engagement and support safe harbor, such as a fixed dollar cap on protected tools and supports provided to patients and enhanced restrictions on marketing and patient recruitment. As proposed, certain categories of entities that are not typically on the front lines of care coordination and pose a higher risk of fraud or abuse, such as pharmaceutical manufacturers and compounding pharmacies, are ineligible to use the new safe harbors for value-based arrangements, outcomes-based payments, and patient engagement and support. Click here for more information about ineligible entities under these safe harbors. Ineligible entities may be able to use other new or modified safe harbors if an arrangement satisfies all applicable conditions.

Subject to definitions and conditions set forth in the regulations in the Final Rule, the final safe harbor regulations protect:

- *Value-Based Arrangements*. Three new safe harbors for certain remuneration exchanged between or among eligible participants in a value-based arrangement that fosters better coordinated and managed patient care:
  - Care Coordination Arrangements to Improve Quality, Health Outcomes, and Efficiency (§ 1001.952(ee));
  - Value-Based Arrangements With Substantial Downside Financial Risk (§ 1001.952(ff)); and
  - Value-Based Arrangements With Full Financial Risk (§ 1001.952(gg)).

These new safe harbors vary by the type of remuneration protected, level of financial risk assumed by the parties, and safeguards included as safe harbor conditions.

- *Patient Engagement and Support*. A new safe harbor (§ 1001.952(hh)) for certain tools and supports furnished to patients to improve quality, health outcomes, and efficiency.
- *CMS-Sponsored Models*. A new safe harbor (§ 1001.952(ii)) for certain remuneration provided in connection with a CMS-sponsored model (as defined in the Final Rule), which should reduce the need for separate and distinct fraud and abuse waivers for new CMS-sponsored models.
- *Cybersecurity Technology and Services*. A new safe harbor (§ 1001.952(jj)) for donations of cybersecurity technology and services.

- *Electronic Health Records Items and Services*. Modifications to the existing safe harbor for electronic health records items and services (§ 1001.952(y)) to add protections for certain related cybersecurity technology, to update provisions regarding interoperability, and to remove the sunset date.

- *Outcomes-Based Payments and Part-Time Arrangements*. Modifications to the existing safe harbor for personal services and management contracts (§ 1001.952(d)) to add flexibility for certain outcomes-based payments and part-time arrangements.

- *Warranties*. Modifications to the existing safe harbor for warranties (§ 1001.952(g)) to revise the definition of "warranty" and provide protection for bundled warranties for one or more items and related services.

- *Local Transportation*. Modifications to the existing safe harbor for local transportation (§ 1001.952(bb)) to expand and modify mileage limits for rural areas and for transportation for patients discharged from an inpatient facility or released from a hospital after being placed in observation status for at least 24 hours.

- *Accountable Care Organization (ACO) Beneficiary Incentive Programs*. Codification of the statutory exception to the definition of "remuneration" under the anti-kickback statute related to ACO Beneficiary Incentive Programs for the Medicare Shared Savings Program (§ 1001.952(kk)).

Subject to definitions and conditions set forth in the regulations in the Final Rule, the final exception regulations under the Beneficiary Inducements CMP protect:

- *Telehealth for In-Home Dialysis*. An amendment to the definition of "remuneration" in the CMP rules at 42 C.F.R. § 1003.110 interpreting and incorporating a new statutory exception to the prohibition on beneficiary inducements for "telehealth technologies" furnished to certain in-home dialysis patients.

Readers are directed to the Final Rule for the regulations we are finalizing and further explanation of the regulations.

APPENDIX “G”

Operating an Effective Compliance Program

- Policies and Procedures
  - Regularly review and update with department managers and Compliance Committee.
  - Assess whether they are tailored to the intended audience and their job functions.
  - Ensure they are written clearly.
  - Include "real-life" examples.

- Measuring Effectiveness
  - Develop compliance program with benchmarks and measurable goals.
  - Set up a system to measure how well you are meeting those goals.
  - Involve the Board in creating the program and regularly update the Board regarding compliance risks, audits, and investigations.
  - If one or more goals are not met, investigate why and how to improve in the future.
  - Assess whether the compliance program has sufficient funding and support.

- Training
  - Regularly review and update training programs. Try different approaches. Use "real-life" examples.
  - Make training completion a job requirement.
  - Test employees' understanding of training topics.
  - Maintain documentation to show which employees received training.
  - Train the Board.
  - Train yourself and your compliance staff. Attend conferences and webinars, subscribe to publications and OIG's email list, monitor OIG's website, and network with peers to stay up-to-date and get ideas.

- Lines of Communication
  - Have open lines of communication between you and employees.
  - Maintain an anonymous "hotline" to report issues to you.
  - Enforce a non-retaliation policy for employees who report potential problems.
  - Establish a direct line of communication between you and the Board.
  - Use surveys or other tools to get feedback on training and on the compliance program.
  - Use newsletters or internal websites to maintain visibility with employees.
  - Regularly meet with the Board and brief them on the compliance program.

- Internal Auditing
  - Perform proactive reviews in coding, contracts & quality of care.
  - Create an audit plan and re-evaluate it regularly.
  - Identify your organization's risk areas. Use your networking and compliance resources to get ideas and see what others are doing.
  - Don't only focus on the money – also evaluate what caused the problem.
  - Create corrective action plans to fix the problem.
  - Refer to sampling techniques in OIG's Self Disclosure Protocol and in CIAs to get ideas.

- Enforcement of Policies and Procedures and Prompt Response to Compliance Issues
  - Delegate/empower teams closest to the issues to perform reviews, but be careful of possible conflicts or personal relationships that may interfere with getting an objective review.
  - Act promptly, and take appropriate corrective action.
  - Create a system or process to track resolution of complaints.
  - Enforce your policies consistently through appropriate disciplinary action.

HEALTH CARE COMPLIANCE PROGRAM TIPS

The Seven Fundamental Elements of an Effective Compliance Program

1. Implementing written policies, procedures and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
6. Enforcing standards through well-publicized disciplinary guidelines.
7. Responding promptly to detected offenses and undertaking corrective action.

Five Practical Tips for Creating A Culture of Compliance

1. Make compliance plans a priority now.
2. Know your fraud and abuse risk areas.
3. Manage your financial relationships.
4. Just because your competitor is doing something doesn't mean you can or should. Call 1-800-HHS-TIPS to report suspect practices.
5. When in doubt, ask for help.

APPENDIX “H”

RECOMMENDED COMPLIANCE RESOURCES

I. OIG Resources

- OIG homepage: http://oig.hhs.gov/

- OIG Fraud Prevention & Detection webpage: http://oig.hhs.gov/fraud.asp
  Provides links to various OIG industry guidance documents (e.g., compliance program guidance, advisory opinions, fraud alerts, special advisory bulletins) as well as links to information on enforcement actions and reporting fraud.

  - OIG's Compliance Program Guidance: http://oig.hhs.gov/fraud/complianceguidance.asp

    Includes compliance program guidance materials for various industry sectors.

  - Corporate Responsibility and Corporate Compliance Guide: http://oig.hhs.gov/fraud/docs/complianceguidance/040203CorpRespRsceGuide.pdf

  - OIG Advisory Opinions: http://oig.hhs.gov/fraud/advisoryopinions.asp

    - Frequently Asked Questions about the Advisory Opinion Process: http://oig.hhs.gov/fraud/advisoryopinions/aofaq.asp

  - OIG's Self-Disclosure Protocol: http://oig.hhs.gov/fraud/selfdisclosure.asp

  - OIG Exclusions: http://oig.hhs.gov/fraud/exclusions.asp

  - Anti-Kickback Safe Harbor Regulations: http://oig.hhs.gov/fraud/safeharborregulations.asp
    Provides the regulatory history of the safe harbors. The current text of all the regulatory safe harbors is available at: http://edocket.access.gpo.gov/cfr_2010/octqtr/pdf/42cfr1001.952.pdf.

  - Medical Identity Theft & Medicare Fraud: http://oig.hhs.gov/fraud/IDTheft/

  - OIG Fraud Hotline: http://oig.hhs.gov/fraud/hotline/ or 1-800-HHS-TIPS

  - OIG Brochure "A Roadmap for New Physicians: Avoiding Medicare and Medicaid Fraud and Abuse": http://oig.hhs.gov/fraud/PhysicianEducation

  - Subscription to OIG's E-mail List with Notifications of New Online Materials: http://oig.hhs.gov/mailinglist.asp

II. CMS and Other Resources

- CMS homepage: http://www.cms.gov/

- CMS Contacts Information Page: http://www.cms.gov/ContactCMS/
  Lists public contact lines for CMS offices and provides a portal for accessing information about CMS national and local operations and key CMS programs.
  - CMS Contacts Database: http://www.cms.gov/apps/contacts/
    Provides access to searchable directories of contacts on national and local levels for the Department of Health and Human Services, CMS offices, Fiscal Intermediaries, and Carriers.
  - CMS Regional Office Overview: http://www.cms.gov/RegionalOffices/
    Provides downloadable files containing CMS Regional Office contact information.

- CMS Physician Self-Referral Law ("Stark Law") Information:
  http://www.cms.gov/PhysicianSelfReferral/
  Provides overview and links to relevant law, regulatory materials, and guidance documents, including a Frequently Asked Questions page.
  - CMS Physician Self-Referral Law Advisory Opinions Library:
    http://www.cms.gov/PhysicianSelfReferral/95_advisory_opinions.asp
    Includes information on requesting CMS Advisory Opinions and links to the CMS Physician Self-Referral Disclosure Protocol, as well as links to a disclosure process overview and relevant background information.

- HIPAA Privacy and Security Rules:
  - http://www.hhs.gov/ocr/privacy/index.html
  - http://www.cms.gov/HIPAAGenInfo/

- National Plan and Provider Enumeration System:
  https://nppes.cms.hhs.gov/NPPES/Welcome.do
  Contains information regarding registering for a National Provider Identifier.

- Homepage for U.S. Departments of Health & Human Services and Justice Joint Campaign against Health Care Fraud: http://www.stopmedicarefraud.gov/

- Website managed by the U.S. Department of Health & Human Services regarding Affordable Care Act: http://www.healthcare.gov/

APPENDIX “I”

Nuvance Health™

2022 Medicare C & D Update

Patient Rights Under HIPAA

Understanding the Nine (9) Key Patient Rights

December 29, 2022

The Nine (9) Key Patient Rights under HIPAA

1. • **Right to Access, Inspect, Obtain, and Transmit a copy of PHI (45 C.F.R. § 164.524[a][1])**
2. • **Right to Amend PHI (45 C.F.R. § 164.526[a][1])**
3. • **Right to Receive an Accounting of Disclosures of PHI (45 C.F.R. § 528 [a][1])**
4. • **Right to Request Restriction of Uses and Disclosures (45 C.F.R. § 164.522[a][1][i])**
5. • **Right to a Copy of the Notice of Privacy Practices for PHI (45 C.F.R. § 164.520[a][1], [c][3])**
6. • **Right to Request Confidential Communications (45 C.F.R. § 164.522[b][1])**
7. • **Right to Receive Notice of Breach (45 C.F.R. § 164.404[a][1])**
8. • **Right to Complain to HHS (45 C.F.R. § 160.306[a])**
9. • **Right to Opt-out of the Patient Directory (45 C.F.R. § 164.510[a][2])**

Patient Right # 1

Right to Access, Inspect, Obtain, and Transmit a Copy of their PHI

- Patients have the right to request access to and inspect (as well as obtain) their own medical records
- Patients have a right to direct the transmission of a copy of their medical record to a designated person or entity
- Requests must be in writing and made to the Director of Health Information Services for hospital records or to the Manager of the medical office location
- The Risk Management Department should also be contacted in the event the patient is a current inpatient and they request access to their records
- Attachment "A" provided additional information regarding patient access, inspection, and transmission rights under HIPAA

Patient Right # 2

Right to Request an Amendment

- Patients have the right to request amendments to their own medical records.

- The organization does not have to agree to the amendment if the record is already accurate and complete.

- Requests for hospital record amendments should be referred to Health Information Management (HIM)

- Requests for other provider amendments should be referred to that office location Practice Manager

Patient Right # 3

Right to an Accounting of Disclosures

- Patients have the right to a summary of all the times that their PHI was disclosed when the disclosure is not for Treatment, Payment, or Health Care Operations; such as those made to law enforcement agencies, the courts, public health authorities

- Requests for an accounting of disclosures must be referred to Health Information Management.

Patient Right # 4

Right to Restriction Request

- Patients have the right to request that Nuvance Health restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.
- Nuvance Health is under no obligation to agree to requests for restrictions.
- If the restrictions are agreed upon, Nuvance Health must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

Patient Right # 5

Right to Confidential Communications

- Nuvance Health must permit patients to request an alternative means or location for receiving communications of PHI. Accommodations must be made, if the request is reasonable.

- For example, a patient may request that the provider communicate through a designated address or phone number.

Patient Right # 6

Right to a Copy of Notice of Privacy Practices (NPP)

- Nuvance Health, and its affiliates are required to provide patients with the Notice of Privacy Practices (NPP) and obtain a signed acknowledgement form.

  - All patients must be given a Notice of Privacy Practices (NPP) at their first visit or upon request.

  - The NPP describes how the organization uses, discloses and protects the patient's PHI. It also informs the patient of their rights with respect to their PHI.

  - Should there be any questions about our Privacy Policy, please contact the HIPAA Privacy and Security Officer at: compliance@nuvancehealth.org or the **Corporate Compliance Hotline: (844) 937-9326**

Patient Right # 7

Right to Receive Notification of a Breach of their PHI

- Patients have a right to receive notification where it has been determined (by Nuvance Health) that their protected health information ("PHI") has been breached
- ***What is a Breach?*** - A "***breach***" is defined as "*the acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI].*"
- All incidents involving the acquisition, access, use or disclosure of PHI in a manner that violates the HIPAA Privacy Rule is presumed to be a breach and requires notification to all affected patients, the U.S. Department of Health and Human Services, and, under certain circumstances, the media unless:
  - An exception to breach notification exists under the Breach Notification Rule; or
  - Based on the performance of a risk assessment and the results thereof, Nuvance Health demonstrates that there is a **low probability** that the PHI has been compromised based on a risk assessment.

Patient Right # 8

Right to Opt Out of the Facility Directory

- The hospital may maintain a facility directory that contains the following information, unless a patient opts out of the directory

  - Patient's name;
  - Patient's location;
  - Patient's condition in general terms (e.g., stable, guarded) that does not indicate the patient's diagnosis or other detailed clinical information; and
  - Patient's religious affiliation (only to members of the clergy).

- The hospital must inform the patient about the information to be included in the director and to whom the information may be released

- The patient has the right to restrict the information or to whom the information is disclosed to and the right to opt out of being included in the directory

Patient Right # 9

Patient Right to File a Complaint with HHS

- In addition to reporting matters to Nuvance Health, patients may directly file complaints with the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR"), which is Federal agency charged with enforcement of the HIPAA Privacy and Security Rules
- OCR follows up with both the individual filing the complaint and the covered entity listed in the complaint to gain additional details
  - Covered Entities are required by law to cooperate with OCR in any complaint investigation
- OCR will attempt to resolve the case with the covered entity by obtaining:
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement
- If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties on the covered entity

Attachment "A"

The Office of the National Coordinator for Health Information Technology and HHS Office of Civil Rights

Guidance on Patient Access-related Rights under HIPAA

(Health IT.gov – *Your Health Information, Your Rights*)

HealthIT.gov

YOUR HEALTH INFORMATION, YOUR RIGHTS

GET IT. CHECK IT. USE IT.

DID YOU KNOW?

8 in 10 individuals who have viewed their medical record online considered the information useful.[1]

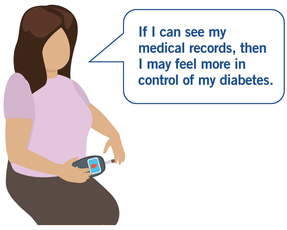
27% of individuals were unaware or didn't believe they had a right to an electronic copy of their medical record.[1]

41% of Americans have never even seen their health information.[2]

HIPAA (Health Insurance Portability and Accountability Act of 1996) gives us the right to access our health information.

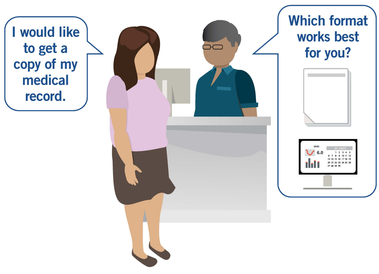
KNOW YOUR RIGHTS

Hannah is a 50-year-old woman recently diagnosed with Type 2 Diabetes.



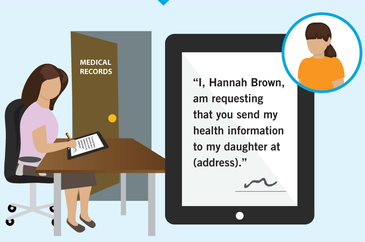
Like all individuals, Hannah has a right to see and get a copy of her health information.

With a copy of your medical record you can become more informed about your health.



SEND YOUR HEALTH INFORMATION TO A THIRD PARTY

You hold the key to your health information and can send or have it sent to anyone you want. Only send your health information to someone you trust.



Your provider is no longer responsible for the security of your health information after it is sent to a third party.

Be careful when sending your health information to a mobile application or other third party.

PROTECT YOUR HEALTH INFORMATION

Sources: 1. https://www.healthit.gov/sites/default/files/briefs/oncdatabrief30_accesstrends_.pdf 2. https://www.healthit.gov/buzz-blog/consumer/making-patient-access-health-information-reality/

LEARN MORE ABOUT YOUR RIGHTS

WWW.HEALTHIT.GOV/ACCESS

www.hhs.gov/hipaa/for-professionals/privacy/guidance/access

The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

APPENDIX "J"

Important Compliance Program-Related Guidance Documents

♦ *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, U.S. Department of Justice (Criminal Division) and U.S. Securities Exchange Commission (Enforcement Division), (2d Ed.) (available at: https://www.justice.gov/criminal/criminal-fraud/fcpa-resource-guide (last accessed on 12-28-23)

♦ U.S. Sentencing Commission Guidelines Manual Section 8B2.1, *Effective Compliance and Ethics Program* (2023) (available at: https://www.ussc.gov/guidelines/2023-guidelines-manual/annotated-2023-chapter-8#8b21) (last accessed on 12-28-23)

♦ U.S. Department of Health and Human Services Office of Inspector General, *General Compliance Program Guidance* (10/23) (available at: https://oig.hhs.gov/compliance/general-compliance-program-guidance/ (last accessed on: 12-28-23)

♦ U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (3/23) (available at: https://www.justice.gov/criminal/criminal-fraud/compliance) (last accessed on 12-28-23)

♦ U.S. Department of Justice, National Security Division, *Export Controls and Sanction Resources* (available at: https://www.justice.gov/nsd/resources) (last accessed on 12-28-23)