ACCOMPANYING GUIDANCE MEMORANDUM- TO BE DOWNLOADED AND PRINTED WHILE REVIEWING VIDEOS

GUIDANCE FOR HEALTH CARE BOARDS AND PRACTITIONERS: PREPARED FOR NORTH HUDSON COMMUNITY ACTION CORPORATION

The following guidance outline/documents have been prepared for you to be read as you watch the videos prepared by the Office of the Inspector General. In accordance with NHCAC policies, reviewing the videos will constitute a portion of your training, which may be completed at your convenience, but no later than January 1, 2022. Also attached is a slide presentation which we ask you to review as well. When you have completed your review of the videos, please execute the below to confirm your completion. If you have any questions regarding the videos, or compliance in general, please feel free to email NHCAC Corporate Counsel: Bart Mongelli Esq. (bmongelli@decotiislaw.com).

Video 1: Boards have the power to enhance compliance of oversight activities and by integrating compliance in a world of new payment models to reduce inefficiency, risk and waste.[1]

There are three critical Board functions in avoiding risks and waste:

1. Compliance of oversight - Board members should be

    a. engaged;
    b. experienced and diverse
    c. informed on risk areas; and
    d. involved and committed to compliance and be adaptable to reimbursement risks.

2. Structuring your compliance program – Consider the following questions:

    a. Does your compliance officer communicate directly to the Board or does he/she have sufficient influence within the organization?
    b. How does your organization encourage communication between compliance staff and the rest of the organization?
    c. Are goals periodically adjusted to account for payment reforms?
    d. How does the Board encourage compliance in day to day activities?
    e. Does the Board hold key employees accountable for compliance with standards?

[1] OIG Video !: Greg Demske, Chief Counsel to the Office of the Inspector General: The above outline is prepared by the NHCC's General Counsel's office as an additional reference to the video material. The outline is not intended to replace the video material nor is it intended to explain the entire subject.

3. Evaluating the effectiveness of standards and processes– Consider the following questions:

   a. What metrics are used to evaluate compliance and how were those methods selected?
   b. How does your organization identify gaps in quality?
   c. Is the organization routinely conducting compliance audits?
   d. Is the organizations response to problems sufficient?
   e. Has your compliance officer identified hurdles to promoting compliance?

Video 2: Exclusion Authorities and Effects of Exclusion[2]

Exclusion – What does it mean and how does it impact your business or employees?

Exclusion is the authority of the OIG to exclude individuals and entities from participation in Medicare, Medicaid, and other Federal health care programs.

The practical effect of exclusion means that no program payments will be made for items or services furnished, ordered or prescribed by the excluded individual or entity. For example, a home healthcare agency cannot employ or contract with an excluded home healthcare aid or they may have to pay back all healthcare payments associated with the work of that aid.

Exclusion impacts an individual's employment by not allowing one to submit a claim to a Federal health care program for items or services furnished by an excluded individual. An excluded individual can do the following in a Federal healthcare setting:

- Work in non-Federal health care program payment settings;
- Provide care to non-Federal health care program beneficiaries;
- There are non-patient care employment options, such as facilities management or graphic design services.

There are two types of exclusion:

1. Mandatory;

   a. when an individual or entity is convicted of a program related crime;
   b. in the instance of conviction relating to patient abuse;
   c. in the instance of a felony relating to a controlled substance; or
   d. in the instance of a felony relating to health care fraud.

2. Permissive – OIG may exclude individuals or entities (under 16 different statutory authorities) for:

[2] Given by: Gita Cavetti, Attorney at the Office of the Inspector General

a. lying on an enrollment application;
b. for certain misdemeanor convictions;
c. loss of state license to practice;
d. failure to repay health education loans; or
e. failure to provide quality care.

How long exclusion lasts varies depending on the case and basis for the exclusion, but the exclusion is typically for a set period of time, except for exclusion for licensure actions which is indefinite. Minimum period for mandatory exclusion is for 5 years and reinstatement is NOT automatic. Rather, one must apply for reinstatement and receive confirmation from the OIG.

Video 3: Federal Anti-kickback statute [3]

Four things every health care provider should know about the Anti-kickback statute:

1. Know what the Anti-kickback statute prohibits;

    a. You may not knowingly or willingly offer or receive anything of value to induce or reward referrals of Federal health care program business;
    b. The law applies to those who pay or receive the kickback.

2. Know the penalties under the law;

    a. Criminal:
        i. Fines – up to $25,000 per violation and/or;
        ii. Felony – up to a 5-year prison term.
    b. Civil:
        Up to three times the government program's loss, plus $11,000 per claim
    c. Exclusion from Federal health care programs;
    d. Up to a $50,000 civil penalty per violation and an assessment of up to three times the total kickback payment, even if some of the payment went to a legitimate purpose.

3. Know the types of programs the law covers – the Law does not apply to all referrals
   The law only applies to Federal health care programs, e.g., Medicare & Medicaid; and

4. Most of you know the law has numerous "safe harbors" – some of these exceptions are:

    a. Employment arrangements;
    b. Space and equipment leases.

[3] Given by: Meredith Williams, Attorney at the Office of the Inspector General

As of December 2, 2020 there are New and Modified Anti-Kickback Statute Safe Harbors

Value-Based Arrangement Exceptions: OIG finalized three new safe harbors for remuneration exchanged between eligible participants in a value-based arrangement that fosters better coordinated and managed patient care. The three value-based safe harbors are similar in some respects but not identical to the Stark exceptions and include:

- Care coordination arrangements to improve quality, health outcomes, and efficiency that does not require the participants to take on risk but protects only in-kind remuneration
- Value-based arrangements with substantial downside financial risk (at least 5%)
- Value-based arrangements with full financial risk for the cost of all items or services covered by a payor for each patient in the target population for a term of one year

Patient Engagement and Support Safe Harbor: OIG finalized a new safe harbor for certain tools and supports furnished to patients to improve quality, health, outcomes, and efficiency.

CMS Sponsored Models: OIG finalized new safe harbor for certain remuneration provided in connection with a CMS-sponsored model, which reduces the need for separate and distinct fraud and abuse waivers for new CMS-sponsored models.

Cybersecurity Technology and Services: OIG finalized a new safe harbor for donations of cybersecurity technology and services essentially the same as the Stark Cybersecurity Exception described above.

Electronic Health Records Items and Services: OIG modified the safe harbor for electronic health records items and services to allow donations of certain related cybersecurity technology to update provisions regarding interoperability, and to remove the December 31, 2021, sunset date.

Outcomes-Based Payments and Part-Time Arrangements: The final rule modifies the AKS safe harbor for personal services and management contracts to add flexibility for certain clinical outcomes-based payments and to eliminate the requirement that part-time arrangements have a schedule of services specifically set out in the agreement.

Warranties: OIG modified the safe harbor for warranties to revise the definition of warranty and provide protection for bundled warranties for one or more items and related services provided they are paid for under the same payment.

Local Transportation: OIG modified the AKS safe harbor for local transportation to expand and modify mileage limits for rural areas (to 75 miles) 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. Ridesharing arrangements are also permissible under this safe harbor.

Accountable Care Organization (ACO) Beneficiary Incentive Programs: The final rule codifies the statutory exception to the definition of remuneration under the AKS related to ACO Beneficiary Incentive Programs for the Medicare Shared Savings Program to allow incentive payments made by an ACO to a beneficiary.

Telehealth for In-Home Dialysis: OIG amended the definition of remuneration in the Beneficiary Inducements Civil Money Penalties statute to incorporate a new statutory exception to the prohibition on beneficiary inducements for "telehealth technologies" furnished to certain in-home dialysis patiways Norris McLaughlin IP Attorneys Volunteer to Judge Higher Education Moot Courts.

Note: An important message here is that what's often a common practice in other industries can be a CRIME when you are talking about Medicare and Medicaid.

Video 4: False Claims Act [4]

[4]The False Claims Act ("FCA") prohibits the submission of false or fraudulent claims to the Government including the Medicare & Medicaid programs.

Claims that may be false include claims where the service:

- Is not rendered;
- Is already covered under another claim;
- Is miscoded;
- Is not supported by the patient's medical record;
- If a claim violates the anti-kickback statutes or the Stark Law.

When the government targets FCA claims, it does not target innocent billing mistakes. False claims are those that the provider knew, or should have known, were false or fraudulent. It is the providers responsibility that claims submitted to Medicare and Medicaid must be true and accurate. However, innocent billing mistakes should be addressed and repaid to the government within 60 days or be subject to penalties.

If a provider fails to comply with the FCA, penalties are up to three times the Government's loss, plus an additional $11,000 per claim (with each occurrence being a separate claim for liability);

The FCA provides incentives to whistleblowers to report fraud by receiving up to 30% of an FCA recovery. Common whistleblowers are:

a. ex-business partners;
b. current or former employees;
c. competitors; or

[4] Given by Katy Fink, Attorney at the Office of the Inspector General

d. patients.

It is important to keep in mind that any person can be a "whistleblower." A whistleblower could be a disgruntled employee, a contractor, a patient, or a vendor.

Video 5: Physician Self-Referral Law[5]

The Physician's Self-Referral Law a/k/a The Stark Law

The Stark Law is intended to prohibit improper referral relationships that can harm the Federal health care programs and program beneficiaries. Improper referral relationships can lead to over-utilization, increased costs and corruption of the medical decision-making process. The Stark Law limits physician referrals of Medicare patients to entities with a financial relationship with the entity. The Law also prohibits those entities from submitting a claim.

How do you know if you violated the Stark Law? There are three basic questions:

1. Is there is a referral from a physician for a designated health service ("DHS"*)? If yes, then

2. Does the physician (or an immediate family member) have a financial relationship with the entity providing the DHS? If yes, then

3. Does the financial relationship fit within an exemption? If no, then you have a Stark Law problem.

Parties that knowingly submit a claim to Medicare in violation of the Stark Law are subject to the following significant penalties:

1. Owing back the entire amount of the claim even if services were rendered and medically necessary;

2. False Claims Act Liability;

3. Civil Monetary Penalties;

4. Program Exclusions

New and Modified Stark Exceptions promulgated as of December 2, 2020

Value-Based Arrangement Exceptions: CMS finalized three new exceptions for value-based arrangements between a physician and an entity that pays physicians based on the quality of patient care delivered rather than the volume of services provided. The value-based exceptions include:

[5] Given by: James Cannoti, Attorney at the Office of the Inspector General

- Full financial risk exception in which the value-based enterprise assumes the full financial risk for the cost of all patient care for each covered patient for a specified time period
- Meaningful downside financial risk exception where the physician is at meaningful downside financial risk (at least 10% of remuneration) for failure to achieve the value-based goals
- Value-based arrangements exception regardless of the level of risk undertaken that permits both monetary and non-monetary remuneration between the parties

Cybersecurity Exception: CMS finalized a new exception that permits the donation to physicians of cybersecurity hardware, software, and services that are necessary and used to implement, maintain, or reestablish cybersecurity. Unlike the existing Stark exception for electronic health records, there is no requirement for the physicians to share in the cost of such hardware or software.

Limited Remuneration Exception: CMS finalized a new exception that permits limited remuneration (not more than $5,000 per calendar year) to a physician including instances where the amount or formula for calculating the remuneration is not set in advance.

Clarification of Commercial Reasonableness, Volume, or Value Standard and Fair Market Value Requirements: CMS's final rule clarifies these three requirements that are found in most of the Stark exceptions. Commercial reasonableness is defined to mean that the arrangement furthers a legitimate business purpose of the parties and is sensible, considering the size, type, scope, and specialty of the parties. It is not based on whether the arrangement is profitable or not. Under the new rule, the amount of compensation will be considered to take into account the volume or value of referrals only when the formula used to calculate compensation includes the volume or value of referrals as a variable that caused compensation to increase or decrease directly with referrals. The new rule further defines fair market value as the value in an arm's length transaction (between a well-informed buyer and seller that are not in a position to refer to each other) consistent with the general market value of the subject transaction.

Indirect Compensation Arrangement Exception: The modifications to this Stark exception provide that the value-based arrangements exceptions will protect a physician's referrals to the entity when an indirect compensation arrangement includes a value-based arrangement to which the physician is a party.

Direct Referrals: CMS added the specific conditions required under the existing special rule for directed referrals (that require patient preference, insurer determinations, and the patient's best medical interest to override any requirement to refer to a specific provider) to the following Stark exceptions: academic medical centers, bona fide employment arrangements, personal services arrangements, physician incentive plans, group practice arrangements with a hospital, fair market value compensation, and indirect compensation arrangements.

Clarification of Set in Advance Requirement: CMS modified the definition of set in advance used in many Stark exceptions to allow modification of compensation during the term of an arrangement (including in the first year) if the modified compensation is not based on the volume or value of referrals. The modification (or formula) must be set forth in writing prior to the furnishing of services but need not remain in place for a year. There is no limit on the number of times that compensation may be modified.

Group Practice Special Rule for Profit Shares and Productivity Bonuses: CMS modified the special rule for profit shares and productivity bonuses to provide that distribution of profits from designated health services directly attributable to a physician's participation in a value-based arrangement are deemed not to take into account the volume or value of the physician's referrals, thereby enabling physicians in a group practice to be rewarded for their participation in a value-based arrangement.

Electronic Health Records: CMS modified the Stark EHR exception to allow donations of cybersecurity software and services, to remove the December 31, 2021, sunset provision, to remove the requirement that donors ensure they are not replacing equivalent EHR technology already owned by physicians, and to allow the physicians to pay their portion of the EHR at reasonable intervals (as opposed to upfront).

*A list of DHSs may be found in the Stark Law Regulations

Video 6: OIG Compliance Program Guidance, Advisory Opinions and other guidance

Where to look for OIG's Guidance – 3 main categories:

1. Compliance Program Guidance ("CPGs")
    a. Provide information on building an effective oversight program and also give overviews of fraud abuse laws and give examples of risk areas that violate these laws;
    b. Organized by industry sector (11 original and 2 supplemental);
    c. the principles and risk areas in the CPG documents can be useful across different industries. E.g., if you are a physical therapy group looking to enter into an arrangement with a nursing home, there are no CPGs for a physical therapy group, but there are CPGs for nursing homes, so the physical therapy group would benefit from a review of the nursing home CPG.
    d. OIG compliance programs in the CPGs refer to principles and suggested practices and do not set forth specific programs. Principles should be tailored to your circumstances.

2. Special Fraud Alerts, Special Advisory Bulletins, and other guidance
    a. Issued when certain trends of abuse are identified and the public and industry need to know;
    b. It is important to stay up to date and familiar with guidance as there might be a piece of information that will apply to your organization.

3. Advisory Opinions

   a. Allow parties to seek formal and binding legal guidance from the OIG about specific business arrangements;
   b. Offer legal protection from prosecution for the party that made the request;
   c. Serve as excellent guidance as the OIG applies consistent analysis to specific facts;
   d. Requests may be made in the Frequently Asked Questions section of the OIG website:

      i. Be certain to review the FAQ page to be sure you have met all of the requirements for a submission;
      ii. The more complete the request, the faster the request is processed; and
      iii. OIG will analyze your request to determine if it runs astray from the anti-kickback statutes or other laws governed by the OIG.

For further information, you can go to www.oig.hhs.gov and use the advanced feature in the upper right-hand corner of the web page under the search box.

To keep up to date, you may sign up for newsletters on the OIG website and "Get Email Updates" or follow the OIG on twitter.

Video 7: Compliance Program Basics [6]

Generally, a Compliance Program is a set of internal policies and procedures put into place to allow your organization to comply with the law.

- An organization can help identify and prevent issues by being proactive instead of reactive.

An effective Compliance Program can enhance your organization's operations, improve quality of care and reduce overall costs.

The gold standard of compliance programs is set forth in OIG's Compliance Program Guidance ("CPGs"), which:

- Provide principles to follow when coming up with a program that best suits your organization's needs.
- There is no one particular model program, since every organization is different.

[6] Given by: Heather Westphal, Attorney at the Office of the Inspector General

- There are seven fundamental basic elements to an effective compliance program:

  1. Written policies and procedures – update periodically;
  2. Have a compliance professional keeping up with Federal compliance procedures;
  3. Conduct effective training – educate your employees;
  4. Facilitate communication between the compliance officer and all employees;
  5. Internal Monitoring – conduct audits. A good program will discover issues from time to time;
  6. Enforce your standards – make sure employees are following the program; and
  7. Promptly respond to issues

Video 8: Tips for Implementing an Effective Compliance Program [7]

Steps to Avoid Failure of Compliance Programs and Submission of False Claims to Health Care Programs:

1. Foster a culture of compliance with sufficient resources allocated to compliance;
2. Create useful policies and procedures that are up-to-date and user-friendly;
3. Train your staff by offering training often;
4. Stay current with compliance by attending conferences and using networking;
5. Promote communication by being open and approachable about compliance; and
6. Take appropriate corrective action by acting promptly when issues arise and taking/documenting corrective action; and
7. Track the resolution of complaints and educate yourself on the OIG self-disclosure protocol.

You may also conduct regular audits of coding, contracts and quality of care.

- Don't wait for Medicare to tell you that you are coding incorrectly;
- If you enter into many contracts with physicians, hire a lawyer to make sure you are compliant with anti-kickback law; or
- Investigate the root causes if your quality of care is suffering. Consider hiring a consultant.

Review compliance programs by asking:

1. Are you meeting your benchmarks:

2. Are people using the hotline to report compliance issues; and

3. Are your corrective action plans sufficient.

[7] Given by: Susan Gillen, Attorney at the Office of the Inspector General

Video 9: Importance of Documentation [8]

Proper documentation in patients records and in claims is important for 3 main reasons:

1. Protect Programs;
   a. to pay the correct amount to the right people
2. Protect Patients;
   a. to promote patient safety and quality of care; and
3. Protect Provider
   a. to avoid liability and keep you out of fraud and abuse trouble.

What can you do to ensure that your documentation practices are correct?

Make sure records are complete – Two examples of incomplete records:

E.g., Billing for a procedure when a medical record cannot backup the claim, in an instance, for example, that a certain procedure, an MRI for example, is not reflected on the medical records for a patient on the date of treatment. The processor will not be able to determine whether the procedure was ordered that the results were read or even used in the patient's treatment. Make sure records are complete.

E.g. Billing under the guise of a diagnosis, when there is no evidence of the diagnosis in the patient's records. Editing notes at a later date to justify coverage can be an issue.

The OIG website is a great resource to review documentation practices to assure there are no issues with claims.

Video 10: Updated OIG Self-Disclosure Protocol [9]

What to do when you discover conduct that may violate the federal fraud and abuse laws? The video sets forth the procedures for the Board in general, but in any instance involving a question of self-disclosure, whether it be fraud and abuse, self-referral, stark laws, and or overpayment, the General Counsel's office should be consulted PRIOR to the institution of any investigation.

The OIG video explanation offers that the institution can use the Provider Self-Disclosure Protocol, which includes timely, corrective action, including self-disclosure being a key element of an effective compliance program. Undertaking self-disclosure demonstrates a culture of

[8] Given by: Julie Tateman, Chief Medical Officer for the US Department of Health and Human Services at the Office of the Inspector General
[9] Given by: Tony Meva, Attorney at the Office of the Inspector General

compliance. In a disclosure, you are able to work collaboratively with the government towards resolution, since such a provider is in a very different position as a provider under investigation because of a whistleblower complaint or other leads. Keeping federal healthcare program payments that a provider should not have can create additional liability under the federal False Claims Act and the Civil Monetary Penalties Law.

What should the Board do in consultation with the General Counsel:

1. Clarify the issue and determine if it is a potential fraud issue;
2. The OIG itself encourages individuals and institutions/corporations to consult with a healthcare attorney who has Federal health care program experience;
3. Decide where to disclose. This is very important since there are various avenues to choose.

OIG suggests in its video that disclosures may be made on the OIG website. Of course, such disclosures should –if decided to be made—only be made after careful review and consultation with the General Counsel's office. Common disclosures are:

1. Billing for items or services furnished by excluded individuals;
2. Evaluation and Management Services and DRG Upcoding;
3. Duplicate billing;
4. Alteration or falsification of records; and
5. Kickback and Stark Law violations.

How to make your protocol resolution go smoothly:

1. Timing – internal investigation and damages calculation wither needs to be finished or you need to commit to being done within 3 months of your submission;
2. Full description of the conduct;
3. Respond promptly for more requests for information.

The plan is to end the with a Settlement Agreement. Either a:

1. DOJ & OIG False Claims Act Settlement; or
2. OIG Civil Monetary Penalties law settlement.

In recognition of coming forward and disclosing conduct, OIG gives two incentives:

1. Pay a lower settlement amount; and
2. No CIA required when provider has fully cooperated.

Video 11: How to Report Fraud to the OIG[10]

Just because your competitor is skirting the law, it does not mean you can or should do the same thing.

What can you do:

1. Report what you are seeing to 1-800-HHS-TIPS; or

2. Report it online at: www.oig.hhs.gov and click the large red button in the upper left-hand corner that says "Submit a Complaint"

    a. you need not be absolutely certain that there is a violation. The OIG will determine;

    b. status reports are not available.

    c. you may report anonymously.

Video 12: Guidance for Health Care Boards

Given by: Greg Demske, Chief Counsel to the Office of the Inspector General

Boards have the power to enhance compliance of oversight activities and by integrating compliance in a world of new payment models to reduce inefficiency, risk and waste.

Three critical Board functions in avoiding risks and waste:

1. Compliance of oversight - Board members should be
    a. engaged;
    b. experienced;
    c. informed on risk areas; and
    d. involved and committed to compliance and be adaptable to reimbursement risks.

2. Structuring your compliance program – Consider the following questions:
    a. Does your compliance officer communicate directly to the Board or does he/she have sufficient influence within the organization?
    b. How does your organization encourage communication between compliance staff and the rest of the organization?
    c. Are goals periodically adjusted to account for payment reforms?
    d. How does the Board encourage compliance in day to day activities?
    e. Does the Board hold key employees accountable for compliance with standards?

3. Evaluating the effectiveness of standards and processes– Consider the following questions:
    a. What metrics are used to evaluate compliance and how were those methods selected?
    b. How does your organization identify gaps in quality?

[10] Given by: Spencer Turnbul, HEAT Initiative Administrator at the Office of the Inspector General

c. Is the organization routinely conducting compliance audits?
d. Is the organizations response to problems sufficient?
e. Has your compliance officer identified hurdles to promoting compliance?

Health Care providers should be familiar with the material elements of The Health Insurance Portability and Accountability Act – commonly referred to as HIPPA.

The below memorandum is for your review and records:

HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES

Target Audience: Medicare Fee-For-Service Providers

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their health information. You play a vital role in protecting the privacy and security of patient information. This fact sheet discusses:

- The Privacy Rule, which sets national standards for when protected health information (PHI) may be used and disclosed
- The Security Rule, which specifies safeguards that covered entities and their business associates must implement 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; U.S. Department of Health & Human Services (HHS); and, in some cases, the media of a breach of unsecured PHI

HIPAA PRIVACY RULE

The HIPAA Privacy Rule 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” is used in this fact sheet, we are referring to these entities and persons.

The Privacy Rule gives individuals important rights with respect to their protected PHI, including rights to examine and obtain a copy of their health records in the form and manner they request, and to ask for corrections to their information. Also, the Privacy Rule permits the use and disclosure of health information needed for patient care and other important purposes.

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 that relates to all of the following:

- 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

PHI includes many common identifiers, such as name, address, birth date, and Social Security number.

Visit the HHS HIPAA Guidance webpage for guidance on:

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

HIPAA SECURITY RULE

Confidentiality: ePHI is not available or disclosed to unauthorized persons or processes

Integrity: ePHI is not altered or destroyed in an unauthorized manner

Availability: ePHI is accessible and usable on demand by authorized persons

The HIPAA Security Rule specifies safeguards that covered entities and their business associates must implement to protect ePHI confidentiality, integrity, and availability.

Covered entities and business associates must develop and implement reasonable and appropriate security measures through policies and procedures to protect the security of ePHI they create, receive, maintain, or transmit. Each entity must analyze the risks to ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate depends on the nature of the entity's business as well as its size, complexity, and resources. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the ePHI
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce

When developing and implementing Security Rule compliant safeguards, covered entities and their business associates may consider all of the following:

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

Covered entities must review and modify security measures to continue protecting ePHI in a changing environment.

Visit the HHS HIPAA Guidance webpage for guidance on:

- Administrative, physical, and technical safeguards
- Cybersecurity
- Remote and mobile use of ePHI

HIPAA BREACH NOTIFICATION RULE

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals; HHS; and, in some cases, the media of a breach of unsecured PHI. Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

The impermissible use or disclosure of PHI is presumed to be a breach unless you demonstrate there is a low probability the PHI has been compromised based on a risk assessment of at least the following factors:

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

- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated.

Most notifications must be provided without unreasonable delay and no later than 60 days following the breach discovery. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually. The Breach Notification Rule also requires business associates of covered entities to notify the 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, as applicable, must follow HIPAA rules. If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA rules. For the definitions of "covered entity" and "business associate," see the Code of Federal Regulations (CFR) Title 45, Section 160.103.

<u>Covered Entities</u>

The following covered entities must follow HIPAA standards and requirements:

- Covered Health Care Provider: Any provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard, such as:

  Chiropractors
  Clinics
  Dentists
  Doctors
  Nursing homes
  Pharmacies
  Psychologists

- Health Plan: Any individual or group plan that provides or pays the cost of health care, such as:
- Company health plans
- Government programs that pay for health care, such as Medicare,
- Medicaid, and the military and veterans' health care programs
- Health insurance companies

- Health maintenance organizations (HMOs)

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
- Business Associates
- Repricing companies
- Value-added networks

A business associate is a person or organization, other than a workforce member of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. A business associate can also be a subcontractor 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 a covered entity enlists the help of a business associate, then a written contract or other arrangement between the two must:

- Detail the uses and disclosures of PHI the business associate may make

- Require the business associate safeguard the PHI

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

Enforcement

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

Violations may result in civil monetary penalties. In some cases, criminal penalties enforced by the

U.S. Department of Justice may apply. Common violations include:

- Impermissible PHI use and disclosure
- Use or disclosure of more than the minimum necessary PHI
- Lack of PHI safeguards

HIPAA Breach Notification Rule
https://www.hhs.gov/hipaa/for-professionals/ breach-notification

HIPAA Guidance
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance

Medicare Learning Network® Product Disclaimer