OptimaHealth®

# HIPAA FOR PROVIDERS 2022

# Understanding HIPAA Privacy

OptimaHealth

Privacy is a serious matter at Sentara Health Plans. Our members trust us to always keep them safe. This includes their Protected Health Information (PHI) and Personally Identifiable Information (PII). The Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA, requires us to keep members' PHI and PII confidential.

# HIPAA FACTS

OptimaHealth

- HIPAA first went into effect in 1996.
- It is enforced by the Office for Civil Rights, a department of Health and Human Services (HHS).
- The HITECH Act was enacted in 2009 and implemented breach notification, Business Associate responsibilities, and penalties.
- HIPAA allows HHS to impose penalties for failure to comply with the HIPAA and/or HITECH regulations.
- Penalties can, and do, go into the millions of dollars.
- HHS can also impose Corrective Action Plans (CAP) that may last years and may cost as much or more than the penalty.

# What is PHI/PII

OptimaHealth

- PHI, short for Protected Health Information, is defined by HIPAA as any past, present, or future individually identifiable information about a patient.
- PHI comes in many forms, including verbal, paper, electronic, and other formats, all of which must be protected.
- Individually identifiable information includes the following identifiers of a patient/resident/client:

  - name
  - web URL
  - date of birth
  - date of death
  - IP address
  - telephone number
  - voicemail
  - license plate number
  - medical record number
  - photographic image
  - date of service
  - account number
  - SSN
  - email address
  - fax number
  - date of discharge
  - device serial number (implanted device)

# What is PHI/PII

OptimaHealth

**Note:** In addition to the items listed above, HIPAA also considers any other characteristic, alone or in combination, that could uniquely identify the individual by PHI.

Unique characteristics may include:

- job type (e.g., mayor, governor, local media personality, CEO, etc.)
- physical characteristic (e.g., moles, birthmarks, height, hair color, eye color, etc.)
- procedure (e.g., HIPEC is only done at two Sentara locations)
- tattoos, piercings, or other body modifications
- unusual radiology results
- injury type
- diagnosis

# Where Is PHI Stored?

OptimaHealth

- Paper printouts with PHI: spreadsheets, PowerPoints, medical records, labels on prescription bottles and IV bags, handwritten notes, messages to call a patient or family, logbooks, and faxes.
- Electronic devices that create, store, or maintain PHI: CT scanners, EMRs, thumb drives, CDs, emails, phones.
- Audio/Video: voicemails, phone calls on speaker, recording conversations (for business and non-business related reasons).

# Securing PHI

OptimaHealth

**Email:**

- Always encrypt emails that contain PHI.
- Before sending PHI or PII out, know that it will probably be reviewed through IT monitoring software.
- If you email a PowerPoint that has a graph or any spreadsheet data, you are probably sending PHI without knowing it. Always check PowerPoints for embedded data before sending.
- Make sure when emailing PHI to follow the Minimum Necessary Standard: Before hitting reply all, make sure everyone on that email chain really needs to see that info. Especially if you are adding new info that contains PHI.
- Understand that email documents are subject to disclosure in legal proceedings to the same extent as a hard copy and use extreme caution when communicating PHI via email.

# Securing PHI

**Fax:**

- Avoid faxing confidential information.
- Use a fax cover sheet with a disclaimer that provides instructions on what to do if received unintentionally.
- Remove the transmitted material immediately from the fax.

**Phone:**

- PHI is not discussed on non-digital cellular telephones or in locations where conversations may be overheard by unauthorized persons.
- Conduct all conference calls involving member information behind closed doors.
- Enable password protection on your mobile device.
- Never connect to unsecure Wi-Fi.
- Accept mobile phone updates to eliminate vulnerabilities.

# Securing PHI

OptimaHealth

**Computer:**

- Log off when leaving the computer.
- Do not share passwords.
- Turn monitor to ensure it is out of view from others.
- Never connect to unsecure Wi-Fi.

**Paper:**

- Do not leave member information unattended in conference rooms, break rooms, or other public access areas.
- Dispose of paper containing PHI in designated shredding bins; do not put in regular trash.

**Removable Devices:**

- Information that is classified as protected information must be encrypted.

# Business Associates (BAs)

OptimaHealth

- Performs services to/for Sentara Health Plans that involves the use or disclosure of member PHI.
- A Business Associate Agreement (BAA) requires specified written safeguards for PHI.
- A BA must sign a Business Associate Agreement (BAA) with Sentara Health Plans in order to access, use, or disclose PHI.

# Permitted Disclosures

OptimaHealth

HIPAA permits several types of disclosures, although disclosures should be limited to the minimum necessary to accomplish the intended purpose of the disclosure. Permitted disclosures include the following:

- **To the individual:** You may disclose PHI to the individual who is the subject of the information.
- **Treatment, payment, healthcare operations:** You may disclose PHI for the treatment activities, payment activities, or healthcare operations of any healthcare provider if the provider has or had a relationship with the individual, and the PHI pertains to the relationship.
- **Uses and disclosures with opportunity to agree or object:** Permission may be obtained by asking the individual outright if they agree to the disclosure. For example, if the patient brings a family member to the examination room, you should ask for their permission before you begin discussing their treatment. Where the individual is incapacitated, use your professional judgment to determine if a disclosure is in the best interests of the individual. For instance, it is likely in the best interests of the patient to disclose the incapacitated patient's condition to a spouse or family member who accompanied the patient to the emergency room.

# Permitted Disclosures

OptimaHealth

**Consult with Privacy before disclosing information, even under these exceptions:**

- **Required by law:** PHI must be disclosed if required by law, including by statutes, regulations, or court orders. If you are requested to disclose PHI as a requirement under the law, contact the privacy team to ensure the disclosure complies with HIPAA.
- **Public health activities:** PHI may be disclosed for certain public health activities, including:
  - disclosures to public health authorities authorized to collect PHI for preventing or controlling disease, injury, or disability
  - disclosures to entities subject to FDA regulation that need PHI for adverse event reporting, tracking of products, and post-marketing surveillance
  - notifications to individuals who may have contracted or been exposed to a communicable disease when the notification is authorized by law
  - disclosures to employers for PHI of employees concerning work-related illness or injury because the PHI is needed by the employer to comply with Occupational Safety and Health Administration (OSHA)

  If you are requested to disclose PHI for public health activities, contact risk management or the privacy team to ensure the disclosure is appropriate.

# Psychotherapy Notes

OptimaHealth

- A patient's authorization is required prior to a disclosure of psychotherapy notes for any reason, including a disclosure for treatment purposes to a healthcare provider other than the originator of the notes. Exceptions are mandatory reporting of abuse and mandatory "duty to warn" situations regarding threats of serious and imminent harm made by the patient.
- **The Privacy Rule** defines psychotherapy notes as notes recorded by a healthcare provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record.
- Psychotherapy notes do not include any information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests; nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, or progress to date.

# Substance Abuse

- Regulation 42CFR Part 2 protects information about a member with a current or past diagnosis of substance abuse.
- Except in limited circumstances, a signed Substance Abuse Authorization is required to disclose information. Exceptions: child abuse reporting, court order (not subpoenas), auditing, medical emergencies, and re-disclosure of the minimum amount of patient health information made to contractors, subcontractors, and legal representatives for purposes of payment and healthcare operations.

# HIPAA Violations

OptimaHealth

**HIPAA Violation** is the acquisition, access, use, or disclosure of PHI which is not permitted by the HIPAA Privacy Rule and which compromises the security or privacy of the PHI.

**Unauthorized Disclosure**

- PHI emailed, handed, mailed, or faxed to the wrong person.
- PHI verbally shared with someone who shouldn't receive it via telephone, voicemail, or conversation.
- Losing or misplacing PHI (includes laptop or mobile device loss and documents lost in transit).

**Notifications**

- Providers must report suspected HIPAA violations immediately.
- The Privacy department conducts and/or coordinates all investigations of suspected HIPAA violations.
- The HIPAA regulations state a covered entity has 60 days from the time they knew, or reasonably should have known, about a breach to notify the affected person(s). The 'clock' for those 60 days begins when someone at the covered entity, other than the person(s) who committed the violation, knew of the incident.

# HIPAA Violation Penalties

OptimaHealth

| **TIER 1**<br>$100–$50,000 per violation<br><br>Maximum $25,000 per year | **TIER 2**<br>$1,000–$50,000 per violation<br><br>Maximum $100,000 per year | **TIER 3**<br>$10,000–$50,000 per violation<br><br>Maximum $250,000 per year | **TIER 4**<br>$50,000 per violation<br><br>Maximum $1.5 million per year |
|---|---|---|---|
| Unaware of the HIPAA violation and, by exercising reasonable due diligence, would not have known HIPAA Rules had been violated. | Reasonable cause that the covered entity knew about or should have known about the violation by exercising reasonable due diligence. | Willful neglect of HIPAA Rules with the violation corrected within 30 days of discovery. | Willful neglect of HIPAA Rules and no effort made to correct the violation within 30 days of discovery. |

# Thank You