Compliance Today

HIPAA Uses & Disclosures related to Care Coordination

The HIPAA Privacy Rule allows covered entities to share protected health information (PHI) with each other **without** a member's authorization for the purposes of treatment, payment, and health care operations (TPO).

Covered Entities

The Privacy Rule applies to health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of the Department of Health and Human Services (HHS) has adopted standards under HIPAA (referred to as covered entities).

Health Plans: individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare Advantage and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies).

Health Care Providers: every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.

Health Care Clearinghouses: health care clearinghouses are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa, such as: electronic claims transactions.

Treatment, Payment, and Operations (TPO)

A covered entity may use and disclose PHI for its own TPO activities. A covered entity also may disclose PHI for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

Treatment: the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

Payment: encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations: any of the following activities: (a) quality assessment and improvement activities, **including case management and care coordination**; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f)

business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

Minimum Necessary Standard

Although such disclosures are permitted, they are still subject to the minimum necessary standard. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

Substance Use Disorder (SUD) Records

It is important to note that SUD records do not have the same authorization exceptions for TPO as other PHI. SUD uses and disclosures **always** require authorization by the member.

For more information:

- *Member Privacy: PHI Use and Disclosure* procedure (CO316)
- *Substance Use Disorder Records Use and Disclosure* policy and procedure (CO367)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)

Information Security: Managing Access & MAC Forms

Strong security controls and individual diligence are critical to preventing unauthorized access or disclosure of ePHI. CHPW uses role-based job descriptions and defined PHI Access Level Categories to limit workforce member access to the appropriate level of PHI, required to perform a specific function.

To ensure the appropriate level of access is granted to a workforce member, the hiring manager (or the business owner in the event of a vendor or auditor) is responsible for partnering with their HR Business Partner to complete and submit a *New Hire Move, Add, and Change (MAC)* form located under Quick Links on InsideCHPW **at least five (5) business days prior to the workforce member or contractor start date**.

When there is a change in job function, it is important that the workforce member's access be confirmed or modified based on their job description. The *Change MAC* form should be submitted **at least five (5) business days prior to the workforce member's change in job function**.

When a workforce member separates employment (voluntarily or involuntarily), the manager must submit a *Departure MAC* as soon as a separation date has been

finalized, but **no later than five (5) business days prior to the workforce member's last day of work** (in the case of voluntary separation), **or immediately** (in the case of involuntary separation) noting same-day separation.

Failure to comply with CHPW's MAC form process or any other security policy may result in disciplinary action as described in the policy *Corrective Action and Discipline* (EE204). Disciplinary action may include termination. Legal actions may also be taken if a violation of the law has occurred.

A quick training is available in LearningConnect for people managers to learn about the MAC Form process. This training is not assigned; search for "MAC Form Training" in the catalogue.

For more information:

- *Employee Network and Facility Access Authorization (MAC Form Procedure)* procedure (CO335)
- *Corrective Action and Discipline* policy (EE204)

Breach Notifications & the Importance of Reporting

HIPAA defines breaches as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. An impermissible use or disclosure if PHI is presumed to be a breach unless the covered entity or business associate (BA), as applicable, demonstrates that there is a low probability that PHI has been compromised.

A breach of PHI shall be treated as "discovered" as of the first day on which the breach is known to have occurred by CHPW. CHPW shall be deemed to have knowledge of a breach if the breach is known or should have been known, to any person, other than the person committing the breach, who is a workforce member or BA of the organization.

CHPW shall deliver notice to the affected member(s) without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. CHPW shall maintain documentation to prove all notifications were made as required, including evidence demonstrating the necessity of delay (if applicable). There are other reporting requirements based on the number of affected individuals, whether it is a security incident, etc. In addition, the Washington State Health Care Authority requires CHPW to notify them within five days of the date of discovery of a breach.

Workforce members play a critical role in ensuring CHPW can meet its deadlines for reporting requirements. Any CHPW workforce member, contractor, or agent who knows of an impermissible disclosure or acquisition of PHI, or who suspects that one has occurred, **must immediately report** that information to their supervisor and to the Compliance department. Failure to report privacy and security incidents may result in disciplinary action, up to and including termination.

A recent enforcement action highlights the importance of timely reporting. Sentra Hospitals (Sentra) entered into an agreement with HHS Office of Civil Rights (OCR) to pay $2.175 million to settle potential violations of the HIPAA Breach Notification and Privacy Rules for their failure to properly report breaches to the HHS. "HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed," said Roger Severino, OCR Director.

Reporting Impermissible Disclosures

The steps for reporting a privacy incident are as follows:

1. The workforce member completes a Privacy/Security Incident Report form, which can be downloaded from the Compliance page on Inside CHPW: https://inside.chpw.org/departments/compliance (in the "Forms - Resources" section).
2. Email the form to the Compliance department at Compliance.Incident@chpw.org.

If a privacy incident is the result of criminal activity or needs immediate attention, the CHPW workforce member must immediately notify the Compliance department, describe the incident, and submit a completed Privacy/Security Incident Report form.

For more information:

- *Privacy Incidents and Breach Notifications* policy (CO311)
- *HIPAA & Privacy/Security Safeguards Violations* policy (CO325)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Corrective Action and Discipline policy (EE204)*

Cybersecurity: Passwords

For years, strong passwords have been the norm, but as technology continues to improve, so too do the skills of hackers. Over time users are subjected to increasingly complex and exhausting rules (upper, lower, and special characters, numbers, symbols, etc.), increasing length requirements, password rotation requirements, and so on. According to the National Institutes of Standards and Technology (NIST), these requirements have essentially taught users to create highly complex passwords that are hard for humans to remember but are easy for computers to figure out and have created habits such as using predictable, easy-t-guess passwords (P@s$w0rd1, anyone), reusing the same password for multiple accounts, or saving them in spreadsheets or on sticky notes that leave ourselves, and the systems we have access to, vulnerable to attack.

Recommendations from the NIST, and CHPW's own IS&T department, are to move away from complex, hard-to-remember passwords and move to using passphrases. A passphrase is a phrase or sentence instead of a word or set of characters. Most password systems won't allow a space, so users typically capitalize the first letter of each word instead. The key to creating a strong passphrase is to use something that's meaningful to you but that wouldn't be easily guessed. And, the longer is usually the better.

Once a phrase has been selected, utilize elements of strong passwords everyone is already used to such as upper- and lowercase letters, numbers, and symbols. According to the NIST, these types of passphrases of at least 10 characters in length are **over 1 million times stronger** than a typical strong password. To be even more secure, enable multi-factor authentication (also known as MFA, or 2FA (2-factor authentication)) whenever possible.

For more information:

- NIST Special Publication 800-63: Digital Identity Guidelines

Compliance Anonymous Reporting

CHPW provides access to a confidential, anonymous **Compliance Hotline** for workforce members to report instances of suspected or detected non-compliance, potential FWA, and other compliance and ethics concerns. The Hotline is operated and available 24 hours a day, seven days a week at **(800) 826-6762**, by

NAVEX (vendor). You can also make an anonymous report online by visiting the Compliance Hotline reporting site at: http://chpw.ethicspoint.com. You can access the online reporting site with the link above, visiting the 'Compliance Hotline' button from the Employee Quick Links on the InsideCHPW home page, and from a link on the Compliance department page on InsideCHPW.

In order to ensure confidentiality and comfort in reporting, the Hotline vendor **does not** trace or record calls. When you make a report online, you are provided with a 'Report Key' and create a password in order to follow up on your report. Without these, you will not be able to follow up on your submission. NAVEX is unable to recover this information for you. If you choose to remain anonymous, no one will attempt to identify you. If you choose to identify yourself, CHPW will keep your identity confidential, to the fullest extent possible or allowed by law.

When you make a report, the information is provided to the VP, Compliance Officer and the VP, General Counsel for investigation and resolution. You can request an update on the progress or outcome of the investigation by contacting the Compliance Hotline and using the unique identification number and PIN provided during your initial report, or by logging in to the online reporting tool using the 'Report Key' and password mentioned above.

Reminders & Updates

Request to Access PHI

Reminder: **all requests to access a member's PHI (whether from the member or a third-party) are forwarded to the Compliance department for vetting and processing.** The Compliance department will reach out to other departments for assistance as needed.

Compliance P&Ps Recently Updated

- *Fraud, Waste, and Abuse* procedure (CO290)
- *Advance Directives* procedure (CO292)
- *CHPW Policy and Procedure Process* procedure (CO305)
- *Member Privacy: PHI Use & Disclosure* procedure (CO316)
- *Responding to Threats of Violence* procedure (CO336)
- *Compliance Audit Procedure* (CO364)