Provider HIPAA Training

CONTRA COSTA HEALTH PLAN

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' protected health information ("PHI") by entities subject to the Privacy Rule. These individuals and organizations, such as providers, are called "covered entities."

PHI includes all "individually identifiable health information."

This Rule ensures that PHI is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public's health and well-being.

HIPAA Security Rule

The Security Rule protects a subset of information covered by the Privacy Rule. This subset is all *electronic protected health information ("e-PHI")* information a covered entity creates, receives, maintains, or transmits in electronic form.

To comply with the HIPAA Security Rule, all covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI
- Detect and safeguard against anticipated threats to the security of the information
- Protect against anticipated impermissible uses or disclosures that are not allowed by the rule
- Certify compliance by their workforce

Covered entities should rely on professional ethics and best judgment when considering requests for these permissive uses and disclosures.

What is a HIPAA Breach?

The acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of PHI.

Did A Breach Occur?

Was medical information involved?

Was the access, use, or disclosure authorized?

Was there a direct need to know or other lawful use? If not, you are required to report as a suspected or actual breach.

Reporting Suspected & Actual HIPAA Breaches

Providers are required to immediately report instances of suspected or actual HIPAA breaches to compliance@cchealth.org

Please consult the Provider Manual and your facility's reporting requirements for further information.

Safeguards Against HIPAA Breaches

Best practices against HIPAA breaches include:

- Do not share passwords to systems containing PHI
- Do not leave devices unsecured and unattended
- Use secure channels of communication
- Dispose of PHI properly
- Access PHI only when appropriate
- Do not hare PHI on social media
- Ensure you complete your annual HIPAA training

Questions?

Contact CCHP Compliance at
compliance@cchealth.org