HIPAA AND HEALTH INFORMATION EXCHANGE

CORHIO™
COLORADO REGIONAL HEALTH INFORMATION ORGANIZATION

Are you wondering how your participation in CORHIO's health information exchange (HIE) fits in with your HIPAA compliance program? Your participation in CORHIO could actually improve your HIPAA program. CORHIO must comply with the same regulations you do when handling patient information. HIE is simply changing the way you already send or receive patient information to and from other health care providers. Instead of using fax machines, paper copies and "snail mail" to exchange information, HIE allows you to use a secure, instantaneous electronic connection.

At CORHIO, we take patient privacy and security of health information very seriously. Not just because it's the law, because it's the right thing to do.

A LITTLE BACKGROUND ON HIE AND HIPAA

CORHIO's HIE makes it possible for providers to access and exchange patient information electronically, improving patient safety and reducing delays in care that can be caused when paper records are illegible, get lost, are accidentally destroyed by fire, flood or natural disaster, or are sent to the wrong fax machine or address. It also helps providers access more complete and up-to-date patient medical records, which is especially helpful in emergency situations or for patients who have a chronic medical condition for which they see many providers over the course of a year.

The CORHIO HIE exchanges lab results, radiology reports, orders, medications, referrals, consult reports, immunizations and other types of clinical health information. All of this information is protected and exchanged under strict privacy and security procedures.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that, in part, calls for protecting the privacy and security of individually identifiable patient information (called "protected health information" or "PHI"). Four HIPAA rules affect HIE – the Privacy Rule, the Security Rule, the Breach Notification Rule and the Enforcement Rule.

In 2009, HIPAA enforcement was expanded to include those who provide services that require access to or interaction with PHI on behalf of HIPAA covered entities (e.g., healthcare providers, health plans) by the Health Information Technology for Economic and Clinical Health (HITECH) Act. These service providers are called "business associates" under the HIPAA statute and regulations. The HITECH Act also specifically defines health information organizations, like CORHIO, to be business associates. This means CORHIO must directly comply with the HIPAA statute and regulations and are subject to civil and criminal penalties, just like providers.

Under HIPAA, HITECH and related regulations, CORHIO follows these guidelines:

- HIEs may use, disclose and request PHI only in relation to their HIE activities and as defined in their agreements with participants.
- HIEs may disclose PHI to subcontractors only if necessary and must hold them to the same standards for privacy and security.

Additionally, CORHIO's policies and participant contracts specify that it will not use or provide PHI obtained through the HIE for marketing, fundraising, underwriting, enrollment/eligibility decisions or pre-existing condition determinations by health plans.

HIEs are responsible for HIPAA compliance and are subject to enforcement by regulators, just like providers.

PATIENT PRIVACY

The HIPAA Privacy Rule defines under what circumstances PHI may be accessed, used or disclosed, what processes must be in place to control access, and how specific patient privacy rights must be supported. In general, the rule is governed by a "minimum necessary" and "need to know" approach so that use and disclosure of

PHI is limited to only the information needed to perform a job function or meet a specific, permitted objective.

CORHIO has strict policies and procedures for handling PHI, including:

- Designated Privacy Officer for oversight of policies and procedures pertaining to the privacy of patient information
- Participant education on CORHIO policies and procedures pertaining to privacy
- Handling and destruction procedures for PHI that needs to be printed
- Regular audits of who accesses PHI
- Annual HIPAA training for all employees

CORHIO audits PHI access by both participants and employees and quickly responds to any suspicion or complaint of misuse or noncompliance.

DATA SECURITY

The HIPAA Security Rule defines the standards that covered entities and business associates must follow in implementing basic security safeguards to protect PHI. Security is the ability to control access and protect electronic information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss. The standards call for administrative, technical and physical safeguards designed to protect the confidentiality, integrity and availability of PHI.

CORHIO has many industry-standard security measures in place, including:

- Designation of an Information Security Officer for oversight of policies and procedures pertaining to the security of patient information
- Usage of a highly secure data center
- Regular facility updates
- Periodic risk assessment
- System monitoring, failover capabilities and backups
- Periodic independent penetration testing by 3rd party
- Anti-virus and other security controls
- Regularly scheduled security updates
- Adherence to data encryption standards from the National Institute of Standards and Technology (NIST)
- Strict controls on users, including password procedures and access restrictions

CORHIO conducts regular audits to support business continuity and HIPAA compliance.

BEHAVIORAL HEALTH & OTHER INFORMATION MAY BE SUBJECT TO SPECIAL PROTECTION

Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of patient information that may be considered particularly private or sensitive to a patient (e.g., alcohol and substance abuse treatment records, psychotherapy notes, items and services paid for out-of-pocket upon patient request). Providers must each determine and identify what information is subject to special protection prior to sharing data through the CORHIO HIE and are responsible for complying with all applicable laws.

MOVING FORWARD

Health Information Exchange is vital to the future of patient care because it increases provider efficiency, minimizes redundant testing and improves clinical decision-making. As providers, hospitals and other health care facilities become more connected, protecting patient privacy is of the utmost importance.

Before you proceed with any change to your practice operations in regards to protected health information, check with your legal counsel to better understand the specific implications for your situation. This information was brought to you by the Colorado Regional Health Information Organization (CORHIO) for information purposes only and does not take the place of expert legal advice.

CORHIO™
COLORADO REGIONAL HEALTH INFORMATION ORGANIZATION

4500 Cherry Creek S. Dr.
Suite 820
Denver, Colorado 80246

720.285.3200 TEL
720.285.3205 FAX