CTSI
TECHNICAL UPDATE
Volume 27 Number 47 | November 21, 2023

# UNDERSTANDING HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996 with the primary goals of ensuring continuous health insurance coverage for people who have lost or changed jobs and lowering costs by standardizing rules for storing and transmitting protected health information (PHI). Part of the act deals with the safety and security of PHI. The Office for Civil Rights (OCR), part of the U.S. Department of Health & Human Services (HHS), offers training for health care organizations on the civil rights, health information privacy, and patient confidentiality laws that they are subject to under HIPAA. The OCR also audits organizations for compliance with HIPAA laws and investigates complaints concerning possible violations.

## WHO MUST FOLLOW THESE LAWS

We call the entities that must follow the HIPAA regulations "covered entities" and they include:

- Health Plans, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- Most Health Care Providers—those that conduct certain business electronically, such as electronically billing your health insurance, including most doctors, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- Health Care Clearinghouses—entities that process nonstandard health information they receive from another entity into a standard electronic format or data content, or vice versa.

In addition, business associates of covered entities must follow parts of the HIPAA regulations. Examples of business associates include:

- Companies that help doctors get paid for providing health care, including billing companies and companies that process health care claims
- Companies that help administer health plans
- People like outside lawyers, accountants, and IT specialists
- Companies that store or destroy medical records

Covered entities must have contracts in place with their business associates, ensuring that they use and disclose your health information properly and safeguard it appropriately.

## WHO IS NOT REQUIRED TO FOLLOW THESE LAWS

Many organizations that have health information about you do not have to follow these laws. Examples of organizations that do not have to follow the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

## HIPAA FINES

HIPAA fines use a tiered system. The OCR may also levy criminal charges in certain instances, adding additional litigation costs to the fines. Penalties like these can be ruinous to small and mid-size organizations, so you must verify that you and any business with whom you might share PHI comply with HIPAA guidelines.

| Penalty Tier | Culpability | Minimum Penalty per Violation | Maximum Penalty per Violation | Annual Penalty Cap |
|---|---|---|---|---|
| Tier 1 | Lack of Knowledge | $137 | $34,464 | $34,464 |
| Tier 2 | Reasonable Cause | $1,379 | $68,928 | $137,886 |
| Tier 3 | Willful Neglect | $13,785 | $68,928 | $137,886 |
| Tier 4 | Willful Neglect (not corrected within 30 days) | $68,928 | $68,928 | $2,067,813 |

**This table was last updated on October 6, 2023, and includes the inflationary updates for 2023.*

## HIPAA GUIDANCE

The HHS provides numerous publications that offer guidance and training on HIPAA regulations at www.hhs.gov/hipaa/index.html. If your organization deals with PHI, take the time to review and assess the security measures used to protect that information. PHI includes 18 unique, personally identifiable information elements, including names, phone numbers, vehicle identifiers, email addresses, and medical records. Educate your employees on what information is and is not protected under HIPAA to limit the risks of data breaches and the accompanying fines.

## WHAT THIS MEANS FOR COUNTIES

County employees who handle PHI should be trained on HIPAA regulations and protections. As a service to our members, CTSI offers a Training Library of relevant, curated films on a wide range of human resources, workplace safety, and other work-related topics at www.ctsi.org. If you would like to learn more about HIPAA, the Training Library offers two films, HIPAA Overview and HIPAA Crash Course, and one webinar on HIPAA Privacy and Security. You may also contact our Loss Control department at (303) 861-0507 for additional training resources.

**County Technical Services, Inc.**
*Technical Updates are available online at ctsi.org*
800 N Grant St, Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832