The key things employers must know about HIPAA law

Compliance is a top concern for small business owners. There is a variety of sensitive data that business owners need to safeguard including proprietary business information, customer data, and employment records. After all, a data breach can have a lot of negative consequences from both a PR and compliance standpoint.

But what happens when employers need to access and store employee health information? You may have heard the term HIPAA thrown around in regard to medical privacy. However, HIPAA is often referenced incorrectly as the general public tends to have a lot of confusion about who HIPAA applies to and what it actually means. This can cause a great deal of confusion for employers. You may or may not have to be HIPAA-compliant depending on your business and industry, but all employers are subject to some regulations on handling employee medical information.

Whether it's a doctor's note for sick leave, health paperwork related to employee benefits, or verification of an employees covid-19 vaccination status, employers need to know how to properly store this personal data. Find out whether HIPAA applies to your business and what you can do to stay compliant when storing health-related employee data.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a law that governs patient privacy in regards to medical records and information. It regulates how a health plan or a covered health care provider may use or share your protected health information with others. HIPAA was created with several goals in mind including improving the portability of health insurance, improving patient privacy, and ensuring that patients are alerted when secuity breaches occur that could impact their private medical information.

HIPAA includes five rules; the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule The Privacy Rule is the one that comes to mind for most people when HIPAA is discussed. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other protected health information (PHI). The HIPAA Security Rule is also commonly referenced, as it sets forth requirements for administrative, physical and technical safeguards to ensure the confidentiality and security of electronic protected health information.

Does HIPAA apply to employment records?

Many people wrongfully believe that HIPAA applies to anyone using your health information. This is actually not the case.

HIPAA only applies to these specific people or entities:

- **Healthcare service providers.** HIPAA applies to every healthcare provider who electronically transmits

health information for claims processing, benefit eligibility inquiries, referral authorization requests, and other transactions covered under the HIPAA Transactions Rule.

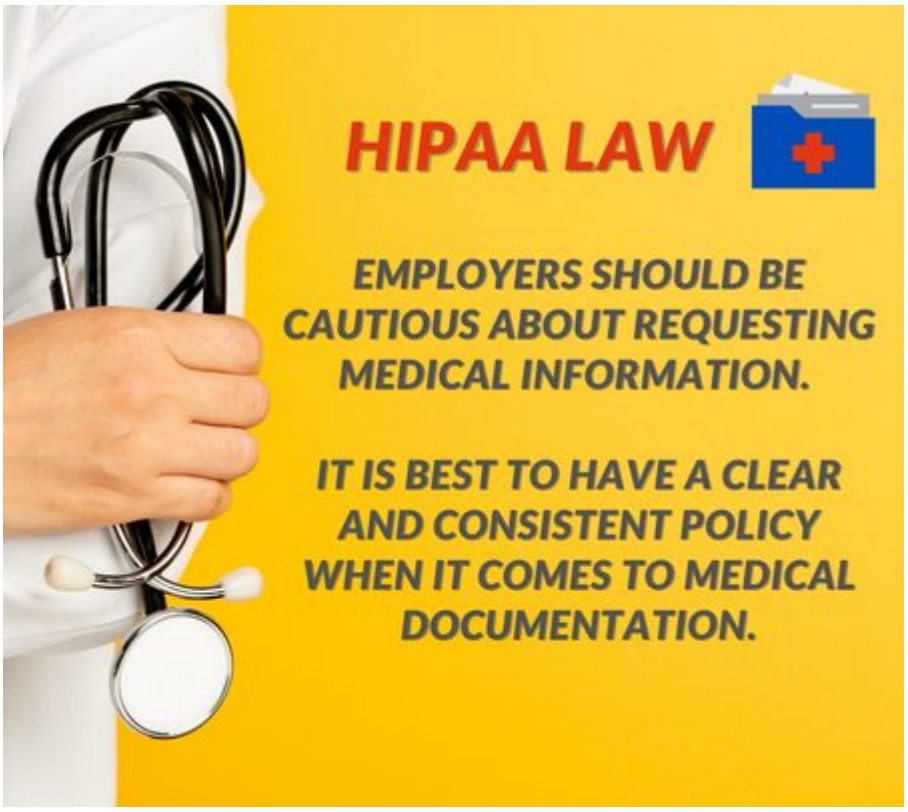
- **Health plans.** Organizations that provide or pay the cost of medical care including health, dental, vision, and prescription drug insurance companies are subject to HIPAA. There is an exception for group health plans with fewer than 50 participants if they are administered solely by the employer.

- **Business associates.** A person or organization using individually identifiable health information to perform or provide services for a covered entity such as claims processing, data analysis, or billing. This can also include healthcare clearinghouses that process healthcare data for HIPAA-regulated organizations.

HIPAA law does not generally apply to employers or protect employment records, even if the employer does collect and store health-relation personal information.

It is worth noting that if you work for a healthcare organization or insurance provider, your employment records are not protected but your patient records are. Employers in these fields should avoid mixing the two and ensure that supervisors and coworkers do not look up an employee's patient records unless they have a legitimate business or patient care need.

Properly storing employee medical information



Employers may not generally be subject to HIPAA regulations, but they do still have some legal responsibilities when it comes to storing employee medical information. The Americans with Disabilities Act (ADA) requires that employee medical records and information be stored separately from an employee's general personnel file. Employers also have a responsibility to maintain confidentiality around any provided employee medical data.

Employers are collecting medical information more frequently than usual now due to the coronavirus pandemic

and safe reopening procedures. If you are collecting vaccination records, health test results, or doctor's notes for illness verification, be sure to store these documents securely and in an ADA-compliant manner.

Examples of employee medical information that should be stored separately from general employment records include:

- Reports of physicals or medical exams conducted as part of a pre-employment screening or following a workplace accident or injury.
- Disability benefits forms.
- Immunization records.
- Doctor's notes.
- FMLA leave paperwork.
- Documentation related to ADA reasonable accommodation requests.
- Health insurance enrollment.
- Referrals from the employee assistance program.
- Worker's compensation claim paperwork.

These documents should only be accessible by employees with a legitimate business use for them such as benefits staff, human resources, or the employee's direct supervisor when necessary.

Can employers request health information?

Yes, employers can request health information in some cases. An employer can ask for a doctor's note or other medical information if it is needed to process sick leave or workers' compensation claims. They may also request health information as part of administering employee wellness programs, FSAs, or health insurance benefits.

However, employers may not directly ask health care providers for information about employees. Health care providers cannot give employers information without the employee's authorization unless other laws require them to do so. Employers should typically make requests for medical documentation to the employee and have them contact their healthcare provider. In this instance, it is actually the provider that is subject to HIPAA and responsible for any resulting HIPAA violations, not the employer.

Employers should be cautious about requesting medical information. It is best to have a clear and consistent policy when it comes to medical documentation. For example, having a policy that a doctor's note is required if an employee is calling out for three or more consecutive days is typically fine. However, issues can arise if you

start asking some employees for notes and not others.

Employers should also be careful to only request the information that they actually need. Inquiring into employees' private medical information, including diagnoses and disabilities, can also raise concerns about discrimination. Doctor's notes should typically focus on what the employee needs in terms of time off or accommodations rather than the employee's specific conditions or illness (unless airborne contagion or safety is an issue such as in the case of covid-19).

Properly disposing of employment records and health information

Holding on to a large backlog of sensitive employee information can be a liability. In addition to having the proper procedures in place for storing health-related information securely in a separate file, it's a good idea to revisit your organization's records retention and disposal procedures.

There are a number of federal laws related to HR record retention, and many of them have specific guidelines for health documentation. Paperwork related to COBRA, employee benefits, OSHA, FMLA, and other medical information all have their own retention schedules and requirements that typically range from 3 to 6 years. Some states also have increased requirements, so it's also a good idea to check your state laws and update your retention schedule at least annually.

It can be hard to keep track of all of these different retention timelines when using paper files. Employers should consider using an electronic method to ensure that files are retained for the appropriate amount of time and then securely disposed of when allowed. This can also cut down on time as paper files will generally need to be shredded before being disposed of if they contact private health information even if HIPAA compliance is not a concern for your business.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002