COMPLIANCE OVERVIEW

Protecting Employees' Medical Information in the Workplace

Employers obtain employees' medical information for various reasons, such as verifying a reasonable accommodation request, certifying leave or confirming eligibility for disability benefits. At the federal level, there are several laws restricting when employers can ask for employees' medical information and requiring employers to keep such information confidential. These laws include the Americans with Disabilities Act (ADA), the Family and Medical Leave Act (FMLA), the Genetic Information Nondiscrimination Act of 2008 (GINA), and the Health Insurance Portability and Accountability Act (HIPAA).

The ADA is the main federal law that protects employees' medical information in the workplace. The ADA limits when covered employers can request employees' medical information (or require medical examinations) and broadly requires all employee medical information to be kept confidential, regardless of why the information was provided. To comply with the ADA, employees' medical information should be maintained separately from personnel files and only accessible to authorized individuals.

State and local laws may impose stricter confidentiality requirements on employees' medical information. Employers should be familiar with the laws for the locations where employees are working and adhere to the strictest applicable requirements.

LINKS AND RESOURCES

- Understanding the ADA: Core Concepts, a resource from the U.S. Equal Employment Opportunity Commission
- FMLA Employer Guide, a U.S. Department of Labor (DOL) publication

Federal Laws

The following federal laws include confidentiality requirements for employees' medical information:

- ADA (applies to all medical information);
- FMLA (applies to leave certifications and family medical history);
- GINA (applies to genetic information, including family medical history); and
- HIPAA (applies to health information from a group health plan, not to employment records).

Compliance Tips

To maintain confidentiality, employers should:

- Use secure storage that is separate from personnel files;
- Limit access to authorized individuals;
- Train employees on confidentiality practices;
- Ensure electronic systems are secure; and
- Promptly address any suspected breaches of confidentiality.

COMPLIANCE OVERVIEW

Quick Overview

Law	Covered Employers	Restrictions on Obtaining Medical Information	Confidentiality
ADA	Employers with 15 or more employees	Prior to a job offer, all medical examinations and disability-related inquiries are prohibited. Applicants may be asked about their ability to perform essential job functions. A job offer may be conditioned on the results of a medical examination, but only if the examination is required for all entering employees in similar jobs. After employment begins, an employer may require medical examinations and make disability-related inquiries only if they are job-related and consistent with business necessity.	With limited exceptions, employers must keep all medical records and information confidential and in separate medical files.
FMLA	Private-sector employers with 50 or more employees and governmental employers of any size	Employers may require employees to provide a health care provider's certification when they request leave for their own serious health condition, the serious health condition of a family member, or the serious injury or illness of a covered service member. In certain circumstances, an employer may also require a fitness-for-duty certification as a condition for returning the employee to their job.	With limited exceptions, employers must keep records relating to medical certifications, recertifications or medical histories of employees or their family members confidential and in separate files.
GINA	Employers with 15 or more employees	Employers cannot request, require or purchase genetic information about applicants or employees, including family medical history, except in very narrow circumstances.	With limited exceptions, employers must keep genetic information about applicants and employees confidential and in separate files.
HIPAA **Does not apply to employment records*	Employers that receive protected health information (PHI) to administer their health plans	Employers can access PHI from their health plan (for example, from a third-party administrator or health insurance issuer) for plan administration purposes if they comply with applicable privacy and security requirements.	The privacy and security of PHI must be protected. PHI from the health plan cannot be used in any employment-related action or decision or in connection with any other benefit plan.

Compliance Tips

In general, employers are required to protect the confidentiality of all employee medical information, regardless of how the information is received or the purpose of the disclosure. The ADA imposes this broad confidentiality protection on employers with 15 or more employees, although other federal laws provide additional protections for specific types of medical information (e.g., genetic information). To keep employees' medical information confidential in accordance with the ADA, employers should consider the following best practices:

- Develop clear policies for the collection, storage, access and use of employees' medical information;
- Maintain medical records in a separate file from the employee's other employment records;
- Use locked cabinets or storage for physical files and secure digital storage for electronic information;
- Limit access to authorized personnel, such as HR personnel;
- Train employees who handle medical information on confidentiality requirements, including the limited situations when information can be disclosed; and
- Promptly respond to any suspected breaches of confidentiality.

ADA

The ADA is a federal law that prohibits employers with **15 or more employees** from discriminating against qualified individuals with disabilities in all employment practices, such as recruitment, compensation, hiring and firing, job assignments, training, leave and benefits. The ADA requires covered employers to provide reasonable accommodations to employees or applicants with disabilities unless doing so would impose an undue hardship on the operation of the employer's business. The ADA also restricts when employers can require employees or applicants to undergo medical examinations or provide disability-related information and imposes confidentiality requirements on employees' medical information.

Restrictions on Obtaining Medical Information

The ADA prohibits covered employers from requiring employees or applicants to **undergo medical examinations or provide disability-related information**, except under certain circumstances. An employer's ability to require medical examinations or make disability-related inquiries is analyzed at three stages: pre-offer, post-offer and employment. These stages are as follows:

- Prior to an offer of employment, all medical examinations and disability-related inquiries are prohibited, even if they are related to the job. An employer may ask job applicants whether they can perform the job and how they would perform the job, with or without a reasonable accommodation;
- After an applicant is given a conditional job offer, but before the individual starts work, medical examinations and disability-related inquiries are allowed regardless of whether they are related to the job as long as they are also required for all entering employees in the same job category; and
- After employment begins, an employer may require medical examinations and make disability-related inquiries only if they are job-related and consistent with business necessity. In general, these standards are met if an employer can show that it has a reasonable belief, based on objective evidence, that the employee's ability to perform essential job functions will be impaired by a medical condition or the employee will pose a direct threat due to a medical condition.

As an exception, medical examinations and disability-related inquiries are permissible after employment begins if they are part of a voluntary wellness program.

Confidentiality

With limited exceptions, the ADA requires employers to treat **any medical information** they receive about an applicant or employee as a **confidential medical record**. This includes health information that employers obtain from a medical examination or disability-related inquiry, as well as any medical information that is voluntarily disclosed by an employee (for example, in connection with a leave request or a request for a reasonable accommodation). Medical information must be treated as confidential even if it does not contain a medical diagnosis or treatment course and even if it is not generated by a health care professional. This ADA protection broadly applies to all applicants and employees, not just those who have a disability.

To maintain confidentiality, the medical information must be kept in **separate medical files** that are only accessible to designated individuals. In addition, health information obtained as part of a voluntary wellness program must be kept confidential. Generally, employers may only receive medical information in aggregate form that does not disclose, and is not reasonably likely to disclose, the identity of specific employees. Also, employers cannot require employees to agree to the sale, exchange, transfer or other disclosure of their health information to participate in a wellness program or receive an incentive.

Employers may only share confidential medical information in the following limited circumstances:

- To supervisors and managers where they need medical information to provide a reasonable accommodation or meet an employee's work restrictions;
- To first-aid and safety personnel if an employee would need emergency treatment or require some other assistance (such as help during an emergency evacuation) because of a medical condition;
- To individuals investigating compliance with the ADA and with similar state and local laws; and
- Pursuant to workers' compensation laws (e.g., to a state workers' compensation office to evaluate a claim) or for insurance purposes.

FMLA

The FMLA is a federal law that provides eligible employees of covered employers with unpaid, job-protected leave for certain family and medical reasons. In general, the FMLA covers private-sector employers with 50 or more employees and governmental employers of any size. Eligible employees may take FMLA leave for the following qualifying reasons:

- The birth of a child and to bond with the newborn child within one year of birth;
- The placement of a child for adoption or foster care and to bond with the newly placed child within one year of placement;
- A serious health condition that makes the employee unable to perform the functions of their job;
- Caring for the employee's spouse, child or parent who has a serious health condition;
- Any qualifying exigency arising out of the fact that the employee's spouse, child or parent is a military member on covered active duty (or call to covered active duty status); and
- Caring for a covered service member with a serious injury or illness if the employee is the spouse, child, parent or next of kin of the service member.

Employers may require employees to provide a health care provider's certification when they request leave for their own serious health condition, the serious health condition of a family member, or the serious injury or illness of a covered service member. Pursuant to a uniformly applied policy, employers may also require that all similarly situated employees provide a certification of fitness to return to work when the absence was caused by their own serious health condition. However, employers that require fitness-for-duty certifications must comply with the ADA requirement that a fitness-for-duty physical be job-related and consistent with business necessity.

Records and documents relating to FMLA medical certifications, recertifications or medical histories of employees or their family members must be treated as **confidential medical records**. Such records must be maintained in **separate files** from the usual personnel files. An employer must maintain these records according to the confidentiality requirements of the ADA and GINA, if applicable. However, supervisors and managers may be informed of necessary restrictions on work duties and necessary accommodations. First-aid and safety personnel may be informed, as appropriate, if the employee's condition might require emergency treatment. Also, government officials investigating compliance with the FMLA (or other pertinent law) must be provided relevant information upon request.

GINA

GINA generally prohibits employers with **15 or more employees** from discriminating against employees or applicants based on their genetic information. More specifically, GINA prohibits the use of genetic information in making employment decisions and restricts employers from requesting, requiring or purchasing genetic information about applicants or employees. GINA also includes confidentiality provisions that strictly limit the disclosure of genetic information.

Genetic information includes information about an individual's genetic tests and the genetic tests of an individual's family members. It also includes information about the manifestation of a disease or disorder in an individual's family members (that is, family medical history).

Restrictions on Obtaining Genetic Information

GINA prohibits employers from requesting, requiring or purchasing genetic information about applicants or employees, except in very narrow circumstances. For example, it is illegal for an employer to require an applicant or employee to answer questions about family medical history during an employment-related medical exam, such as a preemployment exam or a fitness for duty exam during employment. There are six very limited circumstances under which an employer may request, require or purchase genetic information:

1. Where the information is acquired inadvertently, such as a situation where a manager or supervisor overhears someone talking about a family member's illness;
2. As part of a health or genetic service, such as a wellness program, that is provided by the employer on a voluntary basis;
3. In the form of family medical history to comply with the certification requirements of the FMLA, state or local leave laws, or certain employer leave policies;
4. From sources that are commercially and publicly available, including newspapers, books, magazines and electronic sources (such as websites accessible to the public);
5. As part of genetic monitoring that is either required by law or provided on a voluntary basis; and

6. By employers who conduct DNA testing for law enforcement purposes as a forensic lab or for human remains identification.

Also, when an employer asks for information about an applicant's or employee's current health status (for example, to support an employee's request for reasonable accommodation under the ADA or a request for FMLA leave), it should warn the employee not to provide genetic information. This warning is included on the DOL's model FMLA certification forms.

Confidentiality

Employers must keep genetic information about applicants and employees **confidential,** and if the information is in writing, they must keep it apart from other personnel information in **separate medical files**. Genetic information may be kept in the same files as other medical information in compliance with the ADA. There are six limited circumstances under which an employer may disclose genetic information:

1. To the employee or family member about whom the information pertains upon receipt of the employee's or family member's written request;
2. To an occupational or other health researcher conducting research in compliance with certain federal regulations;
3. In response to a court order, except that an employer may disclose only the genetic information expressly authorized by the order;
4. To government officials investigating compliance with Title II of GINA, if the information is relevant to the investigation;
5. In accordance with the certification process for FMLA leave or state family and medical leave laws; or
6. To a public health agency only with regard to information about the manifestation of a disease or disorder that concerns a contagious disease that presents an imminent hazard of death or life-threatening illness.

HIPAA Privacy and Security Rules

HIPAA is a broad federal law that protects the privacy and security of personally identifiable health information, which is called PHI. The HIPAA Privacy Rule sets national standards for when PHI may be used or disclosed and gives individuals certain rights with respect to their PHI. The HIPAA Security Rule includes standards for safeguarding electronic PHI. The HIPAA Privacy and Security Rules (HIPAA Rules) apply to covered entities, which include most health care providers, health plans and health care clearinghouses, and business associates that perform functions on behalf of covered entities involving PHI (collectively, regulated entities).

Impact on Employers

Because employers are not HIPAA-regulated entities, they are not subject to the HIPAA Rules when they perform employment-related functions, such as administering leaves of absence or providing reasonable accommodations. Also, the HIPAA Rules do not apply to employment records held by an employer, even if the records include medical information. These records may include, for example, files or records related to occupational injury, leave requests, drug screenings, reasonable accommodation requests and fitness-for-duty examinations.

Also, medical information that an employee or applicant discloses to their employer is generally not subject to the HIPAA Rules, even if it is prepared by a health care provider. However, because most health care providers are regulated entities,

a HIPAA authorization would be required for a health care provider to directly release an employee's or applicant's medical information (e.g., drug testing results) to the employer.

Health Plan Administration

Although employers are not HIPAA-regulated entities, the HIPAA Rules may indirectly regulate employers in their role as health plan sponsors. Some employers, especially those with self-insured health plans, may receive PHI from their third-party administrators or issuers for plan administration purposes (for example, reviewing claims decisions). When an employer has access to PHI for health plan administrative functions, the employer must comply with certain requirements of the HIPAA Rules. For example, the employer must implement appropriate administrative, physical and technical safeguards to protect the privacy and security of PHI and train its workforce on its privacy and security policies. Also, the employer cannot use PHI from the health plan in any employment-related action or decision or in connection with any other benefit plan.