HIPAA ISSUES FOR EMPLOYERS

D. Wesley Newhouse
Newhouse, Prophater & Letcher, LLC
3040 Riverside Dr.
Columbus, OH 43221
(614) 255-5441
(614) 255-5446 (fax)
wnewhouse@npllawyers.com

I. PROTECTED HEALTH INFORMATION.

A. Protected Health Information (PHI).

Any information about past, present or future mental or physical health.

1. The information must be kept by a covered entity.

2. It must be accompanied by identifying information, such as a name or a Social Security number.

3. It can be oral, handwritten or entered into a computer.

B. Minimum necessary rule.

A health care provider must provide only the minimum information necessary to a person who has a permissible need to know, like billing services, insurance companies and the like.

1. It is left to the health care provider to decide what is minimally necessary.

2. This restriction does not apply to the provision of information for treatment purposes.

II. COVERED ENTITIES.

A. Health care providers.

Almost anyone in the business of providing health care who is licensed or regulated by a state is covered by the act. This includes doctors, hospitals, nurses, dentists, pharmacists, counselors and laboratories.

B. Health plans.

This includes anyone who pays for medical care, such as insurers, HMO's, employer-sponsored health plans, Medicare and Medicaid.

C. Health care clearinghouses.

These are billing services, third-party administrators, insurance agents, and others who collect and process health and health-related information.

D. Hybrid entities.

These include employers. They are organizations which provide health care services as part of their business. Examples include employers with self-insured health benefit programs or workplace medical clinics. The portion of the business must comply with HIPAA requirements for the handling of PHI.

III. EMPLOYER CONFIDENTIALITY OBLIGATIONS UNDER HIPAA.

A. Hybrid entity employers.

1. See preceding discussion regarding coverage.

2. Hybrid employers must build "firewalls" between covered portions of the business and those that are not covered, in order to prevent the inadvertent disclosure of PHI.

    a. Password protect databases at the least, and consider keeping entirely separate computer systems and databases.

    b. Physically separate covered and non-covered employees and files.

    c. Avoid having employees in the covered area also have responsibilities in non-covered areas.

B. Employer access to and use of PHI from covered entities.

1. Covered entities can provide the following to an employer:

    a. Whether an employee is enrolled in a health care plan.

    b. Summary information, such as the number of enrollees, premiums paid, number of claims made, and total costs paid.

2. If a covered entity provides an employer with more information, the employer must adopt and adhere to rules that are essentially the same as those applicable to covered entities.

IV. COMMON LAW PRIVACY OBLIGATIONS.

A. Common law origin.

Unlike some states, Ohio has no statute defining general privacy rights. These rights are a function of court decisions, and are therefore a part of the common law.

B. Reasonable expectation of privacy.

The right of privacy hinges on an employee's reasonable expectation of privacy, which can arise from several sources:

1. Common expectations based on social values (don't peek into the shower stall).

2. Employer policies ("Our e-mail system is for the private use of our employees").

3. Statutory and regulatory restrictions (HIPAA defines medical information as protected, and restricts its dissemination and use).

C. Common law protection of medical information.

Long before there was HIPAA, Ohio courts recognized the duty of an employer to maintain the confidentiality of medical information.

D. Privileges.

A privilege is a common law right of an employer to disclose private information, even without the employee's consent.

1. Provision of information to a medical provider.

2. Provision of information to a health plan.

3. Reporting of medical information to the Bureau of Worker's Compensation.

4. Recording occupational injury and illness information on OSHA prescribed forms, and making those forms to parties with a right of access under OSHA laws and regulations.

5. Use of medical information in defense of an employee's claim of bodily injury.

V. PRACTICAL CONSIDERATIONS FOR THE PROTECTION OF PHI.

A. Obtain authorizations.

When in doubt, obtain written authorization from the employee for disclosure of information. While there are circumstances when this is not necessary, it is best to err on the side of caution.

B. Segregate information.

Medical information should go into a separate folder, and the folder should be a distinctive color (red is good). Look the files up. Restrict who can have access.

C. Written "need to know" forms.

When someone wants to access a medical file, have them complete a standard request form, indicating their intended use for the information, and why they are permitted to see the information. Consider requiring employee authorizations.

D. Policy.

Write and disseminate a policy governing privacy of medical information.