Health Insurance Portability and Accountability Act - HIPAA

What is HIPAA and what does it govern?

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Summary of Administrative Simplification Provisions

- In 1996, the Health Insurance Portability and Accountability Act (HIPAA) became law.

- The original purpose of the Act was to make health insurance more "portable" so that workers could take their health insurance with them when they moved from one job to another without losing health coverage.

- The scope of the Act was broadened to require the health care industry to adopt uniform codes and forms to streamline processing and use of health data and claims and contribute to better, more accessible health care for Americans.

- The Act was also broadened to better protect the privacy of people's health care information, and give them greater access to that information.

The Health Insurance Portability and Accountability Act of 1996, known as HIPAA, include important new - but limited - protections for millions of working Americans and their families. HIPAA may:

- Increase an individual's ability to get health coverage for themselves and their dependents if they start a new job;

- Lower an individual's chance of losing existing care coverage, whether he or she has that coverage through a job, or through individual health insurance;

- Help an individual maintain continuous health coverage, and their dependents when changing jobs; and

- Help individual buy health insurance coverage on his or her own if they lose coverage under an employer's group health plan and have no other health coverage available.

Health Insurance Portability and Accountability Act - HIPAA

Among its specific protections, HIPAA:

- Prohibits group health plans from discriminating by denying coverage or charging extra for coverage based on an individual's or family member's past or present poor health;

- Guarantees certain small employers, and certain individuals who lose job-related coverage, the right to purchase health insurance; and

- Guarantees, in most cases, that employers or individuals who purchase health insurance can renew the coverage regardless of any health conditions of individuals covered under the insurance policy.

Why are privacy and confidentiality important?

The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other personal health information.

- It gives individuals more control over their health information.

- It sets boundaries on use and release of health records.
- It establishes appropriate safeguards that health care providers and others must maintain to protect the privacy of health information.

- It holds violators accountable with civil and criminal penalties that can be imposed if they violate individuals' privacy rights.

- And it strikes a balance when public responsibility supports disclosure of some information. For example, to protect public health.

The average health care provider or health plan will do the following under the Privacy Rule:

- Notify individuals about their privacy rights and how their information can be used.

- Adopt and implement privacy procedures for its practice, hospital, or plan.

- Train employees so that they understand the privacy procedures.

- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.

- Secure individual records containing identifiable health information so that they are not readily available to those who do not need them.

Health Insurance Portability and Accountability Act - HIPAA

Depending on their position, employees of the City of Jacksonville working with medical records may work with documents that have medical information and/or identifiable insurance codes and/or other individual identifiers. By law, this information must be handled in a confidential manner. Failure to keep this information confidential could subject both the City and the employee to civil and criminal penalties if the individual's privacy rights are violated.

To protect the City and representatives of the City, employees will be asked to file complaints if they believe that their medical privacy has been violated. Failure to keep health information confidential may result in discipline up to, and including, termination. Penalties apply even if the disclosure was unintentional.

Employees who ask us to discuss medical information with someone else, either in person or over the telephone, will be required to sign a release of information.

What is confidential information?

Confidential medical information such as:

- A medical file
- Medical test results
- Drug test result
- Alcohol test result
- A prescription
- Overheard conversations between a City employee and others in the office area

What makes information identifiable?

Protected Health Information (PHI) is often denoted by a specific set of personal identifiers that any healthcare operation has, or will ever have, on a patient/client/consumer. For example:

- His or her name
- A social security number
- Employee number
- Location (department, division, worksite)
- Home address
- Date of birth
- Telephone or fax number
- Health plan beneficiary number
- Photographs
- Any other unique identifying number, characteristic or code

Health Insurance Portability and Accountability Act - HIPAA

How is patient information used and who is authorized to use it?

Employee medical information is obtained for specific purposes and must be used only for that reason. Employee medical information is stored in a secure medical file and can only be viewed by the employee, or an authorized City employee who has a business necessity.

Procedures for handling Protected Health Information (PHI)

Office conversation, telephone, or voice mail

- Do not talk about anyone's medical information in public areas such as elevators, reception areas, and the restrooms; whether at work or at home.
- If you do not have an office, always play back voice mail messages by holding the receiver to your ear, because the message may contain PHI.
- Your voice mail must be password protected.

Office Mail and Desk Area

- PHI must not be left placed in a public area, including mailboxes.
- When PHI is outgoing mail, it must leave your office in a sealed envelope.

FAX

- When you FAX a PHI make sure that the "HIPAA Confidentiality Statement" is displayed on the cover-sheet.
- Double check the FAX number, call the receiving party to assure that the FAX is expected, and that it will be picked up immediately.
- When a FAX containing PHI is received, it must be obtained quickly and be protected as soon as possible. After receipt, the FAX must be distributed to the proper recipient.

E-Mail

- When sending a message in the course of business containing PHI, the "HIPAA Confidentiality Statement" must be prominently displayed.
- Make sure PHI is not contain anywhere in the chain of forwarded emails when sending e-mails.
- When communicating with more than one individual about his or her PHI, send separate e-mails to each person.
- Your GroupWise (E-mail) must be password protected. Do not share your password with anyone.
- Terminated employees must have their passwords promptly deactivated.

Health Insurance Portability and Accountability Act - HIPAA

PCs. Laptops, PDAs, and Disks

- Never save PHI on your local hard drive.
- If information is received by disk it should be transferred to the permanent medical file paper or electronic as appropriate.
- Use a screen saver that activates if the computer is not in use for 15 minutes and requires a password to log back in.

Notice Statement to be placed on all correspondence:

NOTICE: This message is confidential, intended for the named recipient(s) and may contain information that is (i) proprietary to the sender, and/or, (ii) privileged; confidential and/or otherwise exempt from disclosure under applicable Florida and federal law, including, but not limited to, privacy standards imposed pursuant to the federal Health Insurance Portability and Accountability Act of 1996 ("HlPAA"). Receipt by anyone other than the named recipient(s) is not a waiver of any applicable privilege or an authorization which permits violation of these laws. Thank you in advance for your compliance with this these confidentiality requirements.