

HIPAA

The Health Insurance Portability and Accountability Act

HIPAA

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses the [privacy of protected health information](#) (PHI) in health care organizations.
- This regulation allows for [civil and criminal penalties](#) for failure to meet the requirements of the privacy regulation or inappropriately disclosing or using confidential health information.
- Employees receive [training on HIPAA policies and procedures](#) when hired and on an annual basis.
- All PHI is to be handled in accordance with Lexington Clinic's policies and procedures on HIPAA.
- If you have questions regarding the release of confidential information or PHI, check with your manager, supervisor, or the Compliance Officer.

HIPAA

- On September 23, 2009, the federal government implemented **new rules** related to HIPAA.
- These rules **mandate** that physicians, and other healthcare providers and vendors, notify patients when their protected health information (PHI) is breached.
- The rules also mandate that we **report all HIPAA breaches** to the Secretary of Department of Health and Human Services annually. Breaches involving more than 500 patients must be reported to the local media.
- In the course of performing your duties at Lexington Clinic, it may be necessary to acquire and record personal, medical, and financial information about our patients. You may also have exposure to other non-medical confidential information relevant to your department.
- All of this information is to be regarded as strictly confidential. Medical records may not be released to anyone other than authorized Lexington Clinic personnel and referring, attending, or consulting physicians without the express written consent of the patient.

HIPAA

- Questions or requests for release of medical information should be directed to the [Release of Information Department at Lexington Clinic](#).
- Other confidential information may only be released in accordance with department guidelines or with permission from your supervisor.
- Great care should be taken to [prevent inadvertent release of confidential information](#) as well. For example, medical charts should be kept out of view of the public.
- As a Lexington Clinic employee, you have a legal and ethical obligation to protect the privacy of our patients. You are not permitted to discuss information regarding a patient with anyone, even your family or other Lexington Clinic employees. When or if you enter the system as a patient of Lexington Clinic, you are entitled to the same rights and privileges regarding the confidentiality of your medical and other records.
- Please note that Lexington Clinic employees [may not access their own medical or other records](#) or those of their spouses, children (regardless of age) or other family members.

HIPAA – Lexington Clinic Policy

Viewing your own records or those of a minor:

1st Offense – Written Letter of Counseling

2nd Offense – 3 Day Unpaid Suspension

3rd Offense – Termination

Viewing medical records of any other patient not defined above or not for work purposes:

1st Offense – 3 day unpaid suspension as a minimum, but could result in action up to and including termination, even for a first offense.

The reason behind the different sets of rules is that viewing your own medical records is not a HIPAA violation. It is a violation of Clinic policy, but it is not a violation of federal law.

All patients are permitted to obtain copies of their medical records or those of a minor dependent under HIPAA law. Our Clinic policy states that this should be done through our Release of Information Department, but viewing such records is not a violation of federal law.

HIPAA – Violating “Need To Know” Requirement

- ❖ Bottom line, if you “need to know” the information in order to do your job, you are not violating HIPAA. If you do not “need to know”, best bet is to stay out!
- ❖ Telling friends or relatives about patients in medical facility
- ❖ This can be done intentionally or even unintentionally. Be careful!
- ❖ Releasing wrong patient’s information
- ❖ This sometimes happens when two patients have the same name and through a careless mistake. Again, be careful!
- ❖ Not logging off your computer
- ❖ ALWAYS log off of your computer (even if you are just stepping away to go to the restroom or for a short 15 minute break).

HIPAA – Violating “Need To Know” Requirement

- ❖ Discussing PHI in public areas
- ❖ Be careful who is around and where you are when discussing Mrs. Jones’ positive pregnancy test. Mr. Jones may be in the elevator with you and Mrs. Jones may have wanted to surprise him!
- ❖ Improper disposal of PHI
- ❖ Always utilize shred bins for disposing of information containing PHI. Never use regular trash cans.
- ❖ Unprotected storage of PHI
- ❖ Keep laptops and any other mobile device containing PHI locked away when not in use.