



Confidentiality/HIPAA Agreement for Interns/Volunteers/Staff/Observers

All information regarding Family Life Services, its clients, staff and programs is considered confidential. It is expected that all interns, volunteer, staff, and observers will comply with this policy at all times. All client's personal health information is protected under the Health Insurance Portability and Accountability Act. Any unauthorized use of client personal health information is illegal under the HIPAA Act.

While HIPPA protects the health information, this form is to also serve to protect the client's personal and financial information as well.

Additionally, no person is allowed to take pictures or videos of any client at Family Life Services without written or documented consent. Audio recording of any type is also prohibited.

Your signature below indicates that you have been educated on confidentiality/HIPAA, that you understand these laws and policies. Signing also signifies that you agree to comply with the law and policies at all times. If you have any questions regarding confidentiality, please ask the Family Life Services Executive Director.

Attached is a copy of the HIPAA Staff Training, the Confidentiality Policy and Procedure for your review and files. If you have any questions, please ask the Director.

Print Name

Date

Signature

Staff Training for the
Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.¹ To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").¹ The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used.

Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

Who is affected?

All healthcare organizations from large health insurance providers to one physician offices.

Are there penalties for violation of HIPAA?

Yes there are penalties. Civil and criminal penalties for noncompliance up to \$25,000 for multiple violations of the same standard in a calendar year. Up to \$250,000 and/or 10 years imprisonment for knowing misuse of individually identifiable health information.

Confidentiality Policy and Procedure

To preserve the dignity and privacy of Family Life Services clients, to prevent the risk of client discrimination, and to prevent the risk of agency liability, confidentiality policies and procedures will be adhered to by all staff members, volunteers, work-force employees, and clinical students. Client information will be disclosed to persons on a “need to know” basis according to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for the purpose of best serving the client’s needs.

1. At the time of hire all employees/work-force will receive training on HIPAA guidelines, confidentiality policies and procedures. For students or volunteers training will be performed prior to interaction with clients or client’s information.
2. Confidentiality policies and procedures will be reviewed with all staff/ current-active volunteers annually.
3. **Client information will NOT be disclosed in a common area with any unnecessary persons in the room.**
4. **Client information will NOT be disclosed to any other clients.**
5. Client records will be stored in a designated and locked area.
6. Clients’ records will be made available to authorized personnel only.
7. Outside agency disclosure of client information will be provided only with informed written consent of the clients according to HIPAA guidelines.
8. Disclosures of information to outside agencies for client personal health information will be processed through FLS program Case Managers or the Executive Director.
9. All requests from outside agencies for client personal health information will be processed through FLS program Case Managers or the Executive Director for clarification.
10. When staff/volunteers are unsure regarding an issue of confidentiality or a request for information, they are directed to the Executive Director.
11. When leaving an office all staff are directed to close or put away any client personal health information.
12. Front office staff are directed to be sure that no client personal health information is within eyesight of visitors.
13. **Any document that contains any client information and needs to be discarded must be shredded.**
14. **No photographs, video or recording of the clients or the facility is allowed unless directed by the Executive Director/Program Case Managers and without written or documented consent (I.E. formal written, text, email, etc.)**
15. If a violation of confidentiality occurs for those in the PMI program, this violation will be reported to KDHE following their guidelines for reporting.