UAB
The 1917 Clinic
a member of the UAB Health System

Volunteer/Intern Application

Volunteer Services: 205-975-9126
www.uab.edu/1917clinic

Thank you for your interest in serving at the UAB 1917 Clinic.
Please complete all portions of this application.
Return by email: Shirley Selvage shirlee6@uab.edu
By mail: UAB 1917 Clinic, Community Care Building 184, 908 20th Street South, Birmingham, AL 35294-2050
By fax: 205-975-6448

Name: ____

Mailing Address: ____

Home Phone: (_____)_________________________ Cell Phone: (_____)_______________________

E-mail Address: ____________________________________ Date of Birth: ________________________

Emergency Contact Name: _______________________ Phone 1: ________________ Phone 2: _______________

This application is intended to give us an understanding of your background and experience. Volunteers will not be turned away due to lack of experience – we just want to know more about you!

Educational History

Type of School	Name	City, State	Dates Attended	Diploma/Degree/ Current Major
High School				
Vocational or Technical				
College or University				
Graduate School				
Other				

Employment History (approximate dates are fine)

Employer	City, State	Dates	Position

Volunteer History (approximate dates are fine)

Organization	City, State	Dates	Position/Duties

Skills and Interests

Please list three things you do well or enjoy doing. (Examples: good listener, computer skills, organizational skills, learning about HIV research, , talking with people, sharing your story, making presentations)

1. ____

2. ____

3. ____

Please explain why you want to be a volunteer at the 1917 Clinic?

____

____

What days and times could you be available? (Please check all that apply. 1917 Clinic is open 8-5, M-F. Some outreach opportunities are available on nights and weekends as requested.)

Day/Time	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Mornings							
Afternoons							
Evening							

What opportunities are you interested in: (check all that apply)

In Clinic: ___Clinic Host ___ Support Groups: _________ ___ Learn and Lunch
Outreach: ___ (SHAPE) Sexual Health Awareness through Peer Education ___ HIV Testing
___ Tabling at Educational Events
Advisory/Action Boards: ___Patient Advisory Board (PAB) ___Clinical Trials (Research Studies)
___ Prevention (Vaccine/Microbicide) Trials

If you are accepted as a member of the volunteer team, are you able to make an initial commitment of at least six months, four hours per week? (for in clinic volunteers only) _____ Yes ______ No
If no, how much time could you commit? ____

How did you hear about our Volunteer Program? ____

References - Please list two professional references who we may contact.
Note: If you are a patient at the 1917 Clinic please include at least one member of your healthcare team (provider, nurse, social worker, counselor).

Name of Reference	E-mail / Phone	Relationship

____ __________
Signature certifying all information is correct and granting permission to verify answers. **Date**

Date received: _________________ Start date: ________________ Position: _______________________

Volunteer Agreement

(for volunteers, interns, and other experiential learning students)

- I agree to adhere to the 1917 Clinic's Confidentiality Policy which states that I will not discuss or acknowledge any identifying factors regarding 1917 Clinic consumers, including those receiving medical care/treatment, HIV Testing, or other individuals living with HIV, to anyone outside of the 1917 Clinic.

- I fully understand that the services I provide the 1917 Clinic are to be given without any expectation of personal remuneration or gain of any kind, financial or otherwise.

- I agree to provide considerate and respectful care for any consumer of the 1917 Clinic, without prejudice or discrimination. I agree to provide services in a non-judgmental manner without regard to sexual orientation, gender, race/ethnicity, religion, physical capabilities, educational level, political opinion, residential or socio-economic status.

- I agree to make to an on-going commitment to educating myself about HIV/AIDS related topics through my volunteer placement and by attending clinic and community events as I am able.

- I agree to be receptive to constructive suggestions and supervision. I agree to bring any problems that may arise in the course of my volunteer service directly to the appropriate staff for resolution.

- I agree to abstain from using mind altering substances or alcohol when performing duties for the 1917 Clinic.

- I agree to fulfill my specific volunteer responsibilities to the best of my ability.

Assumption of Risk and Hold Harmless Agreement

For, and in consideration of being permitted to participate as a volunteer at UAB 1917 (HIV/AIDS) Outpatient Clinic, the undersigned, in full recognition that a clinic environment may present various risks to health and safety, assume all the risks and responsibilities of my participation as a volunteer, and any activities undertaken an hereby agree to hold harmless, release, and forever discharge the Board of Trustees of the University of Alabama (the Board), the University of Alabama at Birmingham (UAB), every division thereof, employees, and agents, and the University of Alabama Health System, from any and all claims, demands, and actions, or causes of action, on account of damage to personal property, personal injury or death, which may result from my participation as a volunteer, and which result from causes beyond the control of, and without the gross negligence of the Board and UAB, its officers, employees or agents, and/or the University of Alabama Health System, during the period of my participation as a volunteer at UAB 1917 Clinic.

I have read all the parts of this agreement and have entered this agreement as a volunteer for the 1917 Clinic.

_________________________   _______________________________   __________________
Volunteer Name (Print)   Volunteer Signature   Date

____   ___________________
Signature of Parent/Guardian if Volunteer is under 19 years of age   Date

____   ___________________
1917 Clinic Staff   Date

- If you have completed an online HIPAA Training at UAB, please include your certificate.
- If you have not completed an online HIPAA Training, please complete the test below using the written material provided.

An Introduction to Confidentiality and Privacy under HIPAA
Nursing, Clinical, And Medical Staff/Volunteers Test

Name: ______________________________ ______________________________

Date: ______________________________ Score: ______________________________

□ **1. What area is addressed by HIPAA?**

a. Notice of Privacy Practices
b. Business Associates
b. Protected Health Information
c. All of the above

□ **2. What is considered to be a "covered entity" under HIPAA?**

a. The Kirklin Clinic, Callahan Eye Foundation Hospital, and UAB Hospital
b. Physicians
c. Health plans such as VIVA
d. All of the above

□ **3. What are the two kinds of sanctions under HIPAA?**

a. Criminal Sanctions
b. Civil Sanctions
c. A and B
d. None

□ **4. What organization is charged with enforcing HIPAA's Privacy Regulations?**

a. Joint Commission
b. The Office for Civil Rights in the Department for Health and Human Services
c. The Healthcare Financing Administration
d. The Federal Bureau of Investigation

□ **5. What form of personally identifiable health information is protected by HIPAA's privacy rule?**

a. Paper
b. Electronic
c. The spoken word
d. All of the above

□ **6. The newspaper has reported that someone famous has come to the hospital, and you're curious to know if this is true. Should you ask around or look for records about this person?**

a. Yes
b. No

□ **7. Providers have until April 14, 2004 to comply with the privacy regulations**

a. True

b. False

□ **8. HIPAA's privacy rule covers not just a patient's health-related information, such as his or her diagnosis, but also other identifying demographic information such as social security number and telephone numbers.**

a. True

b. False

□ **9. Which of the following are some common features designed to protect confidentiality of health information contained in patient medical records?**

a. Locks on medical records rooms

b. Passwords to access computerized records

c. Rules that prohibit employees from looking at records unless they have a need-to-know

d. All of the above

□ **10. A friend is concerned because his girlfriend is in the hospital. He asks you to find out anything you can. Should you try to find information for your friend?**

a. Yes

b. No

□ **11. When is the patient's authorization to release information required?**

a. When patient information is going to be shared with anyone for reasons other than treatment, payment, or healthcare operations

b. To release psychotherapy notes

c. Both A and B

□ **12. You are working elsewhere in the hospital when you hear that a neighbor has just arrived in the ER for treatment after a car crash. You should**

a. Contact the neighbor's spouse to alert him or her about the accident

b. Do nothing and pretend you don't know about it

c. Tell the charge nurse in the ER that you know how to reach the patient's spouse and offer the information if needed

□ **13. If you suspect someone is violating the organization's privacy policy, you should**

a. Confront the individual involved and remind him or her of the rules

b. Watch the individual involved until you have gathered evidence against him or her

c. Report you suspicions to your immediate supervisor of the organization's privacy or compliance officer, as outlined in your organization policy

□ **14. For nurses, physicians and clinical staff who intentionally misuse a patient's protected health information, the penalty is**

a. Fines up to $100

b. Fines up to $25,000

c. Fines up to $250,000 and/or imprisonment for a term up to 10 years

d. None of the above

□ **15. Protected Health Information (PHI) is considered confidential if it is related to:**

a. A person's past, present or future physical or mental health condition

b. A patient's present condition only

c. A patient's past and present *condition only*

UAB
The 1917 Clinic
a member of the UAB Health System

Confidentiality Agreement
UAB 1917 Clinic & Division of Infectious Diseases

Full Name: ____

Degree(s) earned: ____

□ Resident □ Fellow □ New Hire □ Student / Intern □ Volunteer □ Visitor

IMPORTANT: Read all sections. If you have any questions, please ask them before signing. A copy of this signed agreement will be kept on file at the 1917 Clinic and the Division of Infectious Diseases.

DISCLOSURE OF PATIENT/PROVIDER INFORMATION

I recognize that the services provided by the University of Alabama Health Services Foundation, P.C. (UAHSF) and the University of Alabama at Birmingham for its patients are private and confidential; that to enable the UAHSF/UAB to perform those services, patients furnish information to the UAHSF/UAB with the understanding that it will be kept confidential and used only by authorized persons as necessary in providing these services; that the good will of the UAHSF/UAB depends on keeping services and information confidential; that certain legal obligations attach to this information; and that by reason of my duties or in the course of my employment I may receive or have access to verbal, written, or electronic media information concerning patients and services performed by the UAHSF/UAB even though I do not furnish the services performed for those patients.

I hereby agree that, except as directed by the UAHSF/UAB or by legal process, I will not at any time, during or after my employment or during my duties at the UAHSF/UAB, disclose any such services or information to any unauthorized person, or permit any such person to examine or make copies of any reports or other documents prepared by me, coming into my possession or control, or to which I have access, that concerns in any way the patients of the UAHSF/UAB. I agree that I will not attempt to use any information for my own advantage.

I recognize that the unauthorized disclosure of the information by me may violate state or federal laws and do irreparable injury to the UAHSF/UAB or to the patient, and that the unauthorized release of information may result in disciplinary action or dismissal.

SECURITY OF UAHSF INFORMATION/EQUIPMENT

I agree that I will comply with all security regulations in effect at the UAHSF/UAB.

I understand that all software used on a computer owned by the UAHSF/UAB must be properly licensed and approved by UAHSF/UAB Administration for use on that computer. The use of unlicensed or unapproved software constitutes a serious risk to UAHSF/UAB operations. If I use or allow to be used any unlicensed or unapproved software on a UAHSF/UAB computer, I will be subject to disciplinary action or dismissal.

If I have received a sign-on code allowing me to use a computer for UAHSF/UAB business, I agree that I will not disclose and will protect the information and property of the UAHSF/UAB.

I have read all of the above sections of this agreement and I understand them.

SIGNATURE: ______________________________ DATE: ______________

SIGNATURE OF WITNESS: ______________________________ DATE: ______________

UAB/UABHS HIPAA
Privacy and Security Training

What is HIPAA?

- The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996. Although HIPAA addresses issues ranging from health insurance coverage to national standard identifiers for healthcare providers, the portions that are important for our purposes are those that deal with **protecting the privacy and security of health data**, which HIPAA calls **protected health information** or **PHI**

What is PHI?

- **Protected health information (PHI)** is any information, including demographic information, that is **TRANSMITTED** or **MAINTAINED** in any **MEDIUM** (electronically, on paper, or via the spoken word) that is created or received by a health care provider, health plan, or health care clearing house that relates to or describes the past, present, or future **physical or mental health condition** of an individual or past, present, or future **payment for the provision of healthcare** to the individual, and that can be used to identify the individual.

Types of Data Protected by HIPAA

- Written documentation and all paper records
- Spoken and verbal information including voice mail messages
- Electronic databases and any electronic information, including research information, containing ePHI stored on a computer, PDA, memory card, USB drive, or other electronic media
- Photographic images

PHI Data Elements

The following 18 identifiers of an individual or of relatives, employers, or household members of the individual, are considered PHI:

1. Name
2. Geographic subdivisions smaller than a state (street address, city, county, precinct, zip code, and equivalent geocodes)
3. All elements of dates (except year) including birth date, admission and discharge dates, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security number
8. Medical record number
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/License numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locator (URLs)
15. Internet protocol (IP address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, except as allowed under the re-identification specifications (164.514©)

Any one of these 18 identifiers combined with a reference to a diagnosis or medical condition = PHI.

Enforcement, Penalties, and Fines for Noncompliance

- The Department of Health and Human Services, through the Office for Civil Rights and the Centers for Medicare and Medicaid Services, enforces civil monetary penalties for noncompliance with the HIPAA Privacy Rule and Security regulations.
- Civil penalties include fines up to $100 for each violation and up to $25,000 for identical violations during a calendar year
- The U.S. Department of Justice is responsible for enforcing criminal penalties for noncompliance with the HIPAA Privacy Rule.
- Criminal penalties for “wrongful disclosure” include both large fines of $50,000 to $250,000 and up to 10 years in prison! Examples of wrongful disclosures include accessing health information under false pretenses, releasing patient information with harmful intent, or selling PHI

UAB/UABHS HIPAA Privacy Core Standards

The following **privacy core standards** govern how UAB/UABHS and its workforces shall operate in order to meet the HIPAA Privacy Rule:

- Use and Disclosure of Health Information
- Use and Disclosure of Health Information for Marketing
- Use and Disclosure of Health Information for Fundraising
- Use and Disclosure of Identifiable Health Information for Research
- Patient Health Information Rights

The core standards can be found on the UAB/UABHS HIPAA Website at www.HIPAA.uab.edu/standards.

HIPAA Privacy

- **Privacy** is an individual’s right to keep certain information to himself or herself, with the understanding that their protected health information (PHI) will only be used or disclosed with their permission or as permitted by law.

HIPAA Permitted Uses and Disclosures of PHI

The HIPAA Privacy Rule states that PHI may be used and disclosed to facilitate **treatment, payment, and healthcare operations (TPO)** which means:

1. PHI may be disclosed to other providers for **treatment**
2. PHI may be disclosed to other covered entities for **payment**
3. PHI may be disclosed to other covered entities that have a relationship with the payment for certain **healthcare operations** such as quality improvement, credentialing, and compliance.
4. PHI may be disclosed to **individuals involved in a patient’s care or payment for care** unless the patient objects

Minimum Necessary Standard

When HIPAA permits use or disclosure of PHI, a covered entity must use or disclose only the **minimum necessary** PHI required to accomplish the purpose of the use or disclosure.

The only exception to the minimum necessary standard are those times when a covered entity is disclosing PHI for the following reasons:

- Treatment
- Purposes for which a patient authorization is signed
- Disclosures required by law
- Sharing information to the patient about himself/herself

Work-Related Need to Know

- PHI is to be accessed for **business and/or work-related purposes** only—those purposes that are for treatment, payment of that treatment, or health care operations (TPO).
- Do not discuss PHI outside of work or with other employees **who do not need to know the information to perform their jobs.**
- Do not use your access to look up **your own medical information** or **information on your family, friends, or co-workers**
- Accessing PHI without a work-related need to know is an offense which will lead to disciplinary action, up to and including termination.

A Business Associate Agreement (BAA)…

- Is required before a covered entity can **contract a third party individual or vendor (subcontractor)** to perform activities or functions which will involve the use or disclosure of the covered entity's PHI.
- Binds the third party individual or vendor to the HIPAA regulations when performing the contacted services.
- Must be approved in accordance with the appropriate UAB/UABHS policies and procedures.

Individual employees are **NOT** authorized to sign contracts on behalf of UAB/UABHS.
See the UAB/UABHS HIPAA Website at www.HIPAA.uab.edu.

Required Forms of Documents Used at UAB/UABHS

- Notice of Health Information Practices
- Acknowledgement of Receipt of Notice
- Confidentiality Statement
- Authorization for Use or Disclosure of Information
- Accounting of Disclosures Documentation
- Business Associate Agreements
- Fax Coversheet
- Data Use Agreement

Samples of these documents are available on the UAB/UABHS HIPAA website at www.HIPAA.uab.edu

Other Privacy Safeguards

- Avoid conversations involving PHI in public or common areas such as hallways or elevators
- Keep documents containing PHI in locked cabinets or locked rooms when not in use
- During work hours, place written materials in secure areas that are not in view or easily accessed by unauthorized persons.
- Do not leave materials containing PHI on desks or counters, in conference rooms, or in public areas
- Do not remove any PHI in any form from the designated work site unless authorized to do so by management
- Never take photographs in patient care areas.

HIPAA Security Rule

- Contains 18 standards for administrative physical, and technical safeguards for ePHI
- Enforces the following:
  - **Confidentiality**—Information is accessed only by authorized individuals with the understanding that they will disclose it only to other authorized individuals
  - **Integrity—**Information is the same as in the source documents and has not been altered or destroyed in any unauthorized manner
  - **Availability**—Information is accessible to authorized individuals when they need it

UAB/UABHS HIPAA Security Core Standards

Seven (7) core standards govern how UAB/UABHS and its personnel shall operate in order to meet the HIPAA Security Regulations.

- Information System and Account Management
- Internet and Email Use
- Media Reallocation and Disposal
- Information Systems and Network Access
- Contingency Planning
- Risk Analysis and Management of EPHI
- Security Incident Response

The core standards can be found on the UAB/UABHS HIPAA website at www.hipaa.uab.edu/standards

UAB/UABHS Security
Information System and Account Management

1. Do not share your user account, password, token, and other means of system access with anyone
2. Choose a new password each time your password must be reset. Do not reuse your expired passwords
3. Use strong passwords which are at least six to eight characters long. It is recommended to include upper and lower case alphanumeric characters and/or special characters, i.e. #, @ %, /, ?.
4. Do not use pet names, birthdates, or other easily guessed passwords.
5. If you must write down your password, keep it locked up in your wallet protected like a credit card.
6. Only access PHI for business related purposes.
7. Do not use your system access to look up your own medical information or information on friends, family, or co-workers

UAB/UABHS Security
Workstation Responsibilities

1. Arrange computer screens so that they are not visible by unauthorized persons.
2. Do not install or download any software or hardware without authorization
3. Do not use remote control software (such as PC Anywhere) because it can lead to security breaches
4. Do not disable or interfere with anti-virus or automated patching software.
5. Store sensitive and confidential information securely in a directory on a secure network file server. Information stored on the hard drive (C: drive) of a computer or mobile computing device can be lost or compromised.
6. Do not use mobile devices without appropriate security protection. Ask your information systems representative for help. Mobile devices include hand-held, notebook, and laptop computers as well as personal digital assistants (PDAs) and pocket or portable memory devices (USB memory devices such as flash disks, thumb drives, jump drives, etc).
7. Log off or lock your computer when it is left unattended
8. Log off before allowing co-workers to use your computer

UAB/UABHS Security
Email and Internet Use

1. Do not email PHI. If you have a need to transfer confidential information contact your information systems representative for assistance. There is one exception to the "Do not email PHI" rule: PHI can be transmitted securely via email within or between Groupwise and Central Exchange email addresses; however, Central Exchange email addresses but be confirmed with the AskIT Help Desk.
2. Do not forward your UAB/UABHS email account to another email system (Google, AOL, Charter, Hotmail)
3. do not send or forward non-work related mass emails, junk or chain messages, or inappropriate materials. This is against UAB/UABHS policy
4. Do not use the internet for visiting inappropriate sites
5. Do not participate in online chat rooms or instant messaging from work
6. Do not download file sharing software, i.e. Napster, Kazaa
7. Delete suspicious, unsolicited email messages that come from outside UAB/UABHS especially if they contain attachments with "exe" files
8. Notify your information systems representative immediately if you believe your system access has been compromised
9. Do not use public websites (Google, MS Office) for storing ePHI or research data

UAB/UAB Security
Media Reallocation and Disposal

1. Shred documents containing PHI when no longer needed
2. Dispose of CDs or disks containing PHI by placing them in specially marked secure containers or by physically destroying them
3. Sanitize all disks or other media prior to re-use or appropriately destroy them if no longer used. (To "sanitize" means to eliminate confidential or sensitive information from media by either overwriting the data or magnetically erasing data from magnetic media.)
4. Do not reuse CDs or disks containing PHI until they have first been properly sanitized. NOTE: Deleting a file does not actually remove the data from the media!
5. Contact your information systems representative for assistance with sanitization methods

UAB/UABHS Security
Safeguarding Faxes

- Refrain from sending highly confidential information in a fax
- Double check fax numbers before dialing
- Use the covered entity's approved fax cover sheet that includes confidentiality statement
- Do not include any PHI on the cover sheet
- Limit the PHI to the minimum necessary
- Check confirmation sheets to verify that the transmission was successful and accurate
- Ensure that confidential information is not left on the fax machine

Other Security Safeguards

- Wear your identification badges
- Do not allow unauthorized persons into restricted areas
- Confirm the identity and purpose of individuals entering the work area to provide services, such as machine repair or supply delivery
- Do not disable locks on or prop open security doors
- Do not use your personal portable devices for UAB/UABHS business unless such use is specifically approved by senior management

HIPAA and Research

At UAB/UABHS, research is a **USE** of PHI.

HIPAA Privacy and Security regulations apply to research involving human subjects and:

- Impact the use and disclosure of PHI for research
- Do not replace other federal research regulations; therefore, all existing regulations related to human research remain in effect
- Apply whether or not the research is funded by the government

HIPAA Privacy and Research

Covered entities are permitted to use or disclose PHI for research purposes if the Institutional Review Board (IRB) has **approved** the research and one or more of the following conditions exists:

1. A signed **patient authorization** is recorded
2. The research is **decedent research**
3. The process is **preparatory to research**
4. The research utilized a **Limited Data Set with a Data Use Agreement**
5. The IRB grants a **waiver** for the required patient/participant signed authorization

HIPAA Privacy and Research

- Principal investigators or their designees **should not use their clinical access to search for patient records for potential research participants**
- Physicians who are involved in research activities **may contact only their own patients to recruit for research studies**
- Principal investigators or designated researchers **must provide a copy of the fully executed IRB approval form** to the covered entity holding the data before the data can be released for research
- As a rule, first **contact Health Information Management** for PHI to be used for IRB-approved research protocols.

For more information on Research and HIPAA a link is located on the UAB/UABHS HIPAA website at www.hipaa.uab.edu

Ownership of PHI

UAB/UABHS…

- Have ownership of any and all data used within their units for their mission
- Are the owners of our patients' PHI
- Share the responsibility and accountability of the privacy and security of PHI with each data user and custodian in the UAB/UABHS HIPAA covered entities.

Everyone is Responsible for the Security and Privacy of "protected health information!"

1. **Know** what information is considered confidential and protected
2. **Understand** security and privacy standards
3. **Comply** with UAB/UABHS policies and standards
4. **Refer** requests for copies of medical or billing information to appropriate release of information staff within Health Information Management or Medical Records
5. **Report** suspected or known breaches of confidentiality

What if I suspect a breach?

Report it! Report to any or all of the following:

- Your administrative supervisor
- Your Entity Privacy Coordinator (EPC) or your Entity Security Coordinator (ESC)
- The appropriate information systems helpdesk
- The UAB Office of Corporate Complaince

Detailed contact information is available at the UAB/UABHS website at www.hipaa.uab.edu