Teen Volunteer Application

Centennial Medical Center- 2300 Paterson Street- Nashville, TN 37203
Phone: 615-342-1753 Fax: 615-342-1759

Name____ Age _____ SSN_____________________

Address____

Home Phone________________ Cell ________________ Birthday _____/_____/_____

Email __________________________________School ________________________ Grade ____

Mother's Name _____________________________ Phone _______________ Cell _____________

Address ____

Father's Name ______________________________ Phone _______________ Cell _____________

Address ____

Special needs/ concerns/ serious illness ____

Business Experience:

Employer ______________________ Supervisor _______________________ Phone ___________

Address ____

Working this summer? Y N If yes, anticipated schedule __________________________________

Volunteer Experience:

Organization ______________________ Supervisor ______________________ Phone _________

Address ____

Schedule Preferences:

Preferred days/times _________________________ Length of commitment: 3 mo. 6 mo. Summer

Volunteer area of interest ____

Motivation for volunteering? ____

____

For office use only:

Department Assigned _____________________________________ Start Date _________________

0906

Teen Volunteer Letter of Recommendation

Teen volunteer Application-Centennial Medical Center

All students applying for the teen volunteer program must submit recommendations from two of their current teachers, counselors, pastors, community leadership, etc.
Thank you to these mentors for taking the time to provide this information. If you have any questions, please contact the Volunteer Coordinator at 615-342-1753.

Student Name ________________________________ Grade ________________

Organization _________________________________ Phone ________________

I understand the above noted student is applying to participate in the teen volunteer program at Centennial Medical Center. I believe this student is an ideal candidate to serve as a volunteer in a hospital setting, is responsible, and can provide compassion and mature judgment. I am confident this student will carry out their responsibilities with a high regard for the rules, policies and guidelines that must be strictly adhered to given the nature of healthcare.

Reference 1: Name ________________________Class ______________ Date ___________

Additional Comments ____

____

____

____

Reference 2: Name ________________________Class ______________ Date ___________

Additional Comments ____

____

____

____

Teen Volunteer Agreement

Teen volunteer Application-Centennial Medical Center

As a teen volunteer at Centennial Medical Center, I hereby pledge to the following:

1. To perform my volunteer duties to the best of my ability following orientation procedures.
2. To adhere to Centennial Medical Center's rules, procedures, policies and record-keeping requirements and to maintain absolute confidentiality of patient information and other hospital vital information which I may hear directly or indirectly.
3. To meet time and duty commitments and to provide adequate notice, preferably 24 hour notice, in cases of absence to my area supervisor and then volunteer coordinator.
4. To be punctual and conscientious in fulfilling my duties and accept suggestions gracefully.
5. To conduct myself with integrity, compassion, a positive attitude, respect and exceptional quality with all staff, visitors and patients with whom I come into contact.
6. To take any problems, criticisms or suggestions to my supervisor/ volunteer coordinator.
7. To maintain a clean and professional appearance and to return my badge upon completion of the teen volunteer program.
8. I understand my volunteer role can be terminated as a result of:
   - Failure to comply with rules, policies, procedures and record-keeping.
   - Unsatisfactory attitude, work, commitment or appearance.
   - Any other circumstances deemed contrary to the best interest of Centennial Medical Center.

Teen Volunteer Signature ____________________________________ Date _________________

Parent/Guardian Permission

Requires parent/guardian signature

My son/daughter ___________________________________ has my consent to serve as a teen volunteer at Centennial Medical Center. I will encourage compliance with the rules and regulations. I understand he/she must be at least 15 years of age and will be punctual and committed to set schedule. I am aware that 3 unexcused absences from duty will result in dismissal from the program.

Parent/ Guardian Signature _____________________________________ Date ______________

CENTENNIAL MEDICAL CENTER
TEEN VOLUNTEER- ANNUAL HEALTH INFORMATION

__PLEASE COMPLETE ALL THREE SECTIONS AND SIGN ON THE BOTTOM OF PAGE__

Employee Name: ______________________________ Home Phone: ___________________________
Department: ___Volunteer Services____ Soc. Sec. Number: (last 4 digits) ________________

SECTION 1: TB SCREENING

Past Positive PPD (TB Skin Test): NO ____ YES _____ (see back) Pregnant? (see back)

PPD Skin Test 0.1cc ID in arm: (Must be read by RN or MD between **48-72 hours** of administration)

Date given: _____________ RN or MD signature: __________________________________
Date read: ______________ RN or MD signature: __________________________________

Results: NEGATIVE ________ SIZE _0_mm POSITIVE* ________ SIZE ____mm

***POSITIVE TB SKIN TEST THIS TIME? EMPLOYEE MUST FOLLOW UP WITH THE EMPLOYEE HEALTH NURSE AT 342- 4818**

SECTION 2:

__PARENTAL / GUARDIAN PERMISSION FOR TB TESTING__

Teen Volunteer's Name ____
Last First Middle Initial

Birth date _______- _______- _______
Month Day Year

Centennial Medical Center requires that all employees and volunteers have an annual TB skin test. To fulfill this requirement:

________ I have attached a copy of my son/ daughter's TB skin test results performed within the past year.

________ I give my permission for my son/ daughter, ____, to receive a TB skin test at Centennial Medical Center. I understand that he/ she will need to return two days later to have the results read by the Employee Health or Emergency nursing staff.

PARENT/ GUARDIAN SIGNATURE: __________________________________ DATE ______________

CENTENNIAL MEDICAL CENTER-Teen Application cont.

QUESTIONNAIRE FOR SIGNS/SYMPTOMS OF TUBERCULOSIS

I am unable to take the annual TB skin test because:

_____ I am pregnant

_____ I have a history of a past positive Tuberculin skin test

_____ I have a history of BCG vaccination

_____ I am allergic to the preservative found in the Tuberculin skin test

---

Check YES or NO for the following signs and symptoms of active tuberculosis:

Easy fatigue (Tire easily)	YES ____	NO ____
Anorexia (Decreased appetite)	YES ____	NO ____
Weight loss	YES ____	NO ____
Fever	YES ____	NO ____
Night sweats	YES ____	NO ____
Chronic cough (lasting more than three weeks)	YES ____	NO ____
Sputum production (Cough up phlegm)	YES ____	NO ____
If yes, what does it look like? ____		
Hemoptysis (Blood in sputum)	YES ____	NO ____
Chest pain	YES ____	NO ____
Dyspnea (Shortness of breath)	YES ____	NO ____
Significant exposure to someone with active tuberculosis in the past year	YES ____	NO ____

___________________________	________________________________	_________
Print Name	Signature	Date

Confidentiality and Security Agreement

I understand that the facility or business entity (the "Company") in which or for whom I work, volunteer or provide services, or with whom the entity (*e.g.*, physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information (the "Company"), has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment / assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

13. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.
14. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.
15. I will not discuss Confidential Information where others can overhear the conversation. It is not acceptable to discuss Confidential Information even if the patient's name is not used.
16. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
17. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
18. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
19. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company.
20. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
21. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.
22. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
23. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including e-mail, in order to manage systems and enforce security.
24. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and position screens away from public view.

15. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards.

16. I will:

    d. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).

    e. Use only approved licensed software.

    f. Use a device with virus protection software.

16. I will never:

    a. Share/disclose user-IDs, passwords or tokens.

    b. Use tools or techniques to break/exploit security measures.

    c. Connect to unauthorized networks through the systems or devices.

16. I will notify my manager, Local Security Coordinator (LSC), or appropriate Information Services person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.

The following statements apply to physicians using Company systems containing patient identifiable health information (e.g. CPCS/Meditech):

17. I will only access software systems to review patient records when I have that patient's consent to do so. By accessing a patient's record, I am affirmatively representing to the Company at the time of each access that I have the requisite patient consent to do so, and the Company may rely on that representation in granting such access to me.
18. I will insure that only appropriate personnel in my office will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
19. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.

Signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Employee/Consultant/Vendor/Office Staff/Physician Signature	Facility Name and COID	Date
Employee/Consultant/Vendor/Office Staff/Physician Printed Name	Business Entity Name	

Confidentiality and Security Agreement

I understand that the facility or business entity (the "Company") for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company systems.

General Rules

1. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.

Protecting Confidential Information

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
2. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
3. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards and Company record retention policy.
4. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
5. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
6. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards.

Following Appropriate Access

1. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
2. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Using Portable Devices and Removable Media

1. I will not copy or store Confidential Information on removable media or portable devices such as laptops, personal digital assistants (PDAs), cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so

by my job. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards

2. I understand that any mobile device (Smart phone, PDA, etc.) that synchronizes company data (*e.g.*, Company email) may contain Confidential Information and as a result, must be protected. Because of this, I understand and agree that the Company has the right to:
    a. Require the use of only encryption capable devices.
    b. Prohibit data synchronization to devices that are not encryption capable or do not support the required security controls.
    c. Implement encryption and apply other necessary security controls (such as an access PIN and automatic locking) on any mobile device that synchronizes company data regardless of it being a Company or personally owned device.
    d. Remotely "wipe" any synchronized device that: has been lost, stolen or belongs to a terminated employee or affiliated partner.
    e. Restrict access to any mobile application that poses a security risk to the Company network.

Doing My Part – Personal Security

1. I understand that I will be assigned a unique identifier (*e.g.*, 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
2. I will:
    a. Use only my officially assigned User-ID and password (and/or token (*e.g.*, SecurID card)).
    b. Use only approved licensed software.
    c. Use a device with virus protection software.
3. I will never:
    a. Disclose passwords, PINs, or access codes.
    b. Use tools or techniques to break/exploit security measures.
    c. Connect unauthorized systems or devices to the Company network.
4. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords, positioning screens away from public view.
5. I will immediately notify my manager, Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
    a. my password has been seen, disclosed, or otherwise compromised;
    b. media with Confidential Information stored on it has been lost or stolen;
    c. I suspect a virus infection on any system;
    d. I am aware of any activity that violates this agreement, privacy and security policies; or
    e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

1. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
2. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
3. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Employee/Consultant/Vendor Signature	Facility Name and COID	Date
Employee/Consultant/Vendor Printed Name	Business Entity Name	