Volunteer Application- Adult

Volunteer Department
Centennial Medical Center. 2300 Patterson Street. Nashville. TN 37203
615.342.1753 FAX 615.342.1759

Name_____ SSN _____

Address_____

Home Phone_____ Cell _____ Work _____ Birthday ____/____/____
Optional

Email (required):

Education: circle highest year of completion
Grade 6 7 8 HS 1 2 3 4 College 1 2 3 4 Graduate 1 2 3 4

Completed degree (s) _____ Currently in school where? _____

Business Experience: begin with most recent

Employer _____ Supervisor _____ Phone _____

Address _____

Employer _____ Supervisor _____ Phone _____

Address _____

Volunteer Experience: Begin with most recent

Organization _____ Supervisor _____ Phone _____

Email_____ Address _____

Organization _____ Supervisor _____ Phone _____

Email_____ Address _____

Please list special skills/ hobbies: _____

Do you speak a foreign language? Y N If yes, what language? _____

How/why did you choose our volunteer program? _____

Volunteer area of interest _____ Length of commitment: 3 mo. 6 mo. Other/requirement_____

Motivation for volunteering?_____

Adult Application continued

References: Excluding relatives

Name _____ PH/email _____ Relationship _____

Name _____ PH/email _____ Relationship _____

Name _____ PH/email _____ Relationship _____

Have you ever been convicted of a crime? Y N If yes, please explain _____

_____

Emergency Contacts:

Name _____ Phone _____ Relationship _____

Name _____ Phone _____ Relationship _____

Name _____ Phone _____ Relationship _____

Special needs/ concerns: _____

Schedule Preferences:

Preferred days/ times _____How many days/week_____

Willing to assist with special events Y N Willing to be on-call Y N If so, best days/times _____

Agreement:

I have read the forms and understand an investigative report will be made to include information as to character, general reputation, personal characteristics, criminal history, and verification of social security.
I hereby authorize prior employers to provide such information concerning my employment with them as may be requested, and organizations indicated to release information related to volunteer services provided.

Signature _____ Date _____

Volunteer at Centennial

Are you looking to make a difference?
Do you have time to give?
Are you interested in a career in health care?
If so, then we may have a volunteer opportunity for you at Centennial!

We accept adult volunteers starting at age 18 post-high school and teens ages 15-18 on a limited basis.
A hospital volunteer must complete the following requirements:

- Application form
- Interview with Volunteer Coordinator
- Annual health updates including TB skin test, proof of MMR and chicken pox immunity; flu shots required and usually provided at no cost
- Volunteer orientation
- Provide scheduled weekly service with minimum 3 month commitment

Volunteer opportunities include:

- Patient visitor
- Office support e.g. Bariatrics, Human Resources
- Department support e.g. Emergency, Imaging, Rehab on limited basis
- Unit support
- Rockers
- Mail and flower delivery

Further information is available by calling Laurel Haskamp at 615.342.1753
If you receive voice mail, please leave your name, phone, address with zip code and if requesting an adult or teen application.
You may also email your information to Laurel.Haskamp@HCAHealthcare.com and an application will be mailed to you.

FAX to: 615-342-1759

Mail to:
Volunteer Services
Centennial Medical Center
2300 Patterson Street
Nashville, TN 37203

Hospital volunteering requires a lengthy process and commitment. Other TN volunteer opportunities found at:
www.hon.org
www.VolunteerMatch.org

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	