JFK MEDICAL CENTER
A Teaching Affiliate of the University of Miami Miller School of Medicine

Office Use Only

Flu Vaccine: _____ Graded: _____

Badge Deposit: _____ Entered: _____

2016 Clinical Rotation
Student/Resident Orientation Packet

Name: _____

Complete Address: _____

_____

Phone Number: _____ Email: _____

Name of School: _____

Program: _____

Date of Previous Rotation at JFK MC: _____

Clinical Start Date: _____ Clinical End Date: _____

Clinical Days (eg. M/W) _____ Time: _____

Assigned Department or Unit: _____

Preceptorship?: _____ Unit: _____ Preceptor: _____

Instructors Name and Contact Number: _____

Expected Date of Graduation: _____

Where are you employed and in what capacity?:

_____

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 understand that any Confidential Information, regardless of medium (paper, verbal, electronic, image or any other), is not to be disclosed or discussed with anyone outside those supervising, sponsoring or directly related to the learning activity.
2. 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. Case presentation material will be used in accordance with Facility policies.
3. 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.
4. 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.
5. 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. Whether at the School or at the Facility, such safeguards include, but are not limited to: lowering my voice or using private rooms or areas (not hallways, cafeterias or elevators) where available.
6. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information. I will not access data on patients for whom I have no responsibilities or a need-to-know the content of the PHI concerning those patients.
7. 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.

_____	JFK Medical Center 37969	_____
Signature	Facility Name and COID	Date
_____	_____	_____
Printed Name	Entity Name	Date

EXHIBIT A

STATEMENT OF RESPONSIBILITY

For and in consideration of the benefit provided the undersigned in the form of experience in a clinical setting at **JFK Medical Center** ("Hospital"), the undersigned and his/her heirs, successors and/or assigns do hereby covenant and agree to assume all risks and be solely responsible for any injury or loss sustained by the undersigned while participating in the Program operated by _____ ("School") at Hospital unless such injury or loss arises solely out of Hospital's gross negligence or willful misconduct.

_____ _____

Signature of Program Participant/Print Name Date

_____ _____

Parent or Legal Guardian if Program Participant is under 18/Print Name Date

EXHIBIT B

PROTECTED HEALTH INFORMATION, CONFIDENTIALITY, AND SECURITY AGREEMENT

- Protected Health Information (PHI) includes patient information based on examination, test results, diagnoses, response to treatment, observation, or conversation with the patient. This information is protected and the patient has a right to the confidentiality of his or her patient care information whether this information is in written, electronic, or verbal format. PHI is individually-identifiable information that includes, but is not limited to, patient's name, account number, birthdate, admission and discharge dates, photographs, and health plan beneficiary number.
- Medical records, case histories, medical reports, images, raw test results, and medical dictations from healthcare facilities are used for student learning activities. Although patient identification is removed, all healthcare information must be protected and treated as confidential.
- Students enrolled in school programs or courses and responsible faculty are given access to patient information. Students are exposed to PHI during their clinical rotations in healthcare facilities.
- Students and responsible faculty may be issued computer identifications (IDs) and passwords to access PHI.

Initial each box to accept the Policy

Initial	Policy
	1. It is the policy of the school/institution to keep PHI confidential and secure.
	2. Any or all PHI, regardless of medium (paper, verbal, electronic, image or any other), is not to be disclosed or discussed with anyone outside those supervising, sponsoring or directly related to the learning activity.
	3. Whether at the school or at a clinical site, students are not to discuss PHI, in general or in detail, in public areas under any circumstances, including hallways, cafeterias, elevators, or any other area where unauthorized people or those who do not have a need-to-know may overhear.
	4. Unauthorized removal of any part of original medical records is prohibited. Students and faculty may not release or display copies of PHI. Case presentation material will be used in accordance with healthcare facility policies.
	5. Students and faculty shall not access data on patients for whom they have no responsibilities or a "need-to-know" the content of PHI concerning those patients.
	6. A computer ID and password are assigned to individual students and faculty. Students and faculty are responsible and accountable for all work done under the associated access.
	7. Computer IDs or passwords may not be disclosed to anyone. Students and faculty are prohibited from attempting to learn or use another person's computer ID or password.
	8. Students and faculty agree to follow Hospital's privacy policies.
	9. Breach of patient confidentiality by disregarding the policies governing PHI is grounds for dismissal from the Hospital.

- I agree to abide by the above policies and other policies at the clinical site. I further agree to keep PHI confidential.
- I understand that failure to comply with these policies will result in disciplinary actions.
- I understand that Federal and State laws govern the confidentiality and security of PHI and that unauthorized disclosure of PHI is a violation of law and may result in civil and criminal penalties.

_____ _____

Signature of Program Participant/Print Name Date

_____ _____

Parent or Legal Guardian if Program Participant is under 18/Print Name Date

ACKNOWLEDEMENT AND CONSENT FOR RELEASE OF INFORMATION

I have been informed that Hospital requires a background screening as a prerequisite for student placement, and for staff/faculty responsible for supervision and/or instructors of students.

The student background screening shall include, at a minimum, the following:

Social Security Number Verification;

Criminal Search (7 years or up to 5 criminal searches);

Employment Verification to include reason for separation and eligibility for re-employment for each employer for 7 years;

Violent Sexual Offender and Predator Registry Search;

HHS/OIG List of Excluded Individuals/Entities;

GSA List of Parties Excluded from Federal Programs;

U.S. Treasury, Office of Foreign Assets Control (OFAC), List of Specially Designated Nationals (SDN);

The staff/faculty background screening shall include, at a minimum, the foregoing, and additionally, the following:

Education verification (highest level);

Professional License Verification;

Certification & Designations Check;

Professional Disciplinary Action Search;

Department of Motor Vehicle Driving History, based on responsibilities;

Consumer Credit Report, based on responsibilities.

I hereby authorize School to conduct the background screening, and to disclose the results and copies of any background screening in School's possession to Hospital. I further authorize School to permit Hospital to review any background screenings. I understand that this information will otherwise be held confidential by School and will not become a part of my student record.

I acknowledge that Hospital may make the determination, regarding specific background information, that would disqualify me from participating in the program, and that School is not involved in, and has no control over, that determination. I understand that if I am disqualified from participating in the clinical program as a result of the background screening, I may not be permitted to continue in the Medical Center Campus program in which I am enrolled.

I hereby sign this form voluntarily with the understanding that a background screening is a prerequisite to clinical placement in the program.

Name: _____

Date of birth: _____

Student Number: _____

I have worked, resided or been a student in a State other than Florida, or a country other than the United States, during the past 24 months: Yes_____ No_____

If yes, name of State or Country: _____

_____

Signature/Print Name

EXHIBIT C

Attestation of Satisfactory Background Investigation Report

On behalf of _____ [Name of School], I acknowledge and attest to **JFK Medical Center** ("Facility") that we own, and have in our possession, a background investigation report on the individual identified below. Such background investigation report is satisfactory in that it:

____ does not reveal any criminal activity;

____ does not reveal ineligibility for rehire with any former employer or otherwise indicate poor performance;

____ confirms the individual is not on either the GSA or OIG exclusion lists;

____ confirms the individual is not listed as a violent sexual offender;

____ confirms this individual is not on the U.S. Treasury Department's Office of Foreign Assets Control list of Specially Designation Nationals; and

____ no other aspect of the investigation required by Employer reveals information of concern.

I further attest there are no prior or pending investigations, reviews, sanctions or peer review proceedings; or limitations of any licensure, certification or registration.

This attestation is provided in lieu of providing a copy of the background investigation report.

Identified Individual Subject to the Background Investigation:

_____
Name

_____
Address

_____
Date of Birth

_____
Last 4 Digits of Social Security Number

I also acknowledge and agree to an annual compliance audit by Facility of five percent (5%) or a minimum of thirty (30) such background investigation files as authorized by the subjects under the Fair Credit Reporting Act (FCRA).

_____
Signature of School Representative

_____
Printed Name

_____
[Name of Organization]

Date: _____

2016 Student-Resident Orientation Quiz Answer Sheet

1. A B C D
2. True or False
3. A B C D
4. A B C D
5. A B C D
6. A B C D
7. True or False
8. True or False
9. A B C D E F
10. A B C D
11. A B C D
12. A B C D E F
13. A B C D
14. True or False
15. A B C D
16. True or False
17. A B C D
18. A B C D
19. True or False
20. True or False
21. A B C D
22. A B C D
23. True or False
24. A B C D E
25. True or False
26. A B C D
27. A B C D
28. True or False
29. A B C D
30. A B C D E F
31. A B C D
32. True or False
33. A B C D
34. True or False
35. A B C D
36. A B C D E
37. A B C D E F
38. A B C D
39. A B C D
40. A B C D

HIPAA Compliance Requirement

Students must submit proof of HIPAA training or complete our HIPAA Training and Quiz

1. A B C D
2. Yes or No
3. Yes or No
4. A B C D
5. A B C D
6. A B C D
7. True or False
8. A B C D
9. True or False
10. A B C D E

Acknowledgment

In signing below,

I acknowledge that I have received a copy of JFK Medical Center's Student-Resident Orientation and HIPAA Compliance Requirements and have completed both Quizzes.

I also acknowledge that I have received and read a copy of the "**Substance Use in the Workplace" policy.**

I further acknowledge that I will return the JFK MC Hospital ID badge to the Education Department at the end of my stated rotation date in this packet.

Signature: _____

Printed Name: _____

School: _____

Date: _____

JFK MEDICAL CENTER
A Teaching Affiliate of the University of Miami Miller School of Medicine

Returning Your Badge upon Separation from JFK Medical Center

As a vital part of our security system, a JFK Medical Center identification badge with your name, photo and department will be issued to you on your first day of your rotation. The ID badge is also your electronic key to enter the building and other secured areas as needed. Everyone is required to wear an ID badge in plain view while on JFK Medical Center's campus.

If an ID badge is lost or stolen, it should be reported immediately to the security office, and a replacement obtained. The cost of replacement badges will be the student's responsibility.

Upon separation from your rotation, you are required to return your ***JFK ID badge***. If the badge is not returned, you will forfeit your $20.00 deposit. It is the Student Coordinator's responsibility to ensure the ID badge is returned for destruction before leaving the hospital.

The JFK ID badge is the property of the hospital, administered through the Student Department and may be revoked at any inappropriate use. The ID badge may be used only by the individual to whom it was issued. **Students and residents may not "loan" their ID badge to anyone for any reason.**

ACKNOWLEDGEMENT:
I have read and understand the information provided to me. I agree to comply with the expectations outlined above.

Name: (print clearly): _____

Signature: _____ **Date:** _____

JFK MEDICAL CENTER
A Teaching Affiliate of the University of Miami Miller School of Medicine

Badge # _____ **3/4 ID _____**

JFK MEDICAL CENTER
REQUEST FOR IDENTIFICATION CARD

Name of Employee _____

Badge Type **Student**

Title _____

Department _____

_____ _____
Authorizing person's name – please print **Authorizing person's signature**

_____ _____
Clinical Start Date **Clinical End Date**

I have received one (1) JFK Medical Center identification card on the above listed date. I understand that I must always display it, at eye level, while on JFK Medical Center property. I further understand that this identification card is the property of JFK Medical Center and will be turned in upon my termination of employment.

_____
Student/Instructor/Resident full name-please print

_____
Student/Instructor/Resident signature

New Card ( ) Replacement Card ( )

The first card is issued to the student/Instructor/resident at no charge. Replacement non-reader cards will cost $2.00 for each replacement. Replacement reader cards will cost $10.00 for each replacement. Excessive replacements will result in notification to the employee's supervisor.