

December 14, 2011

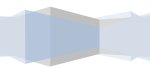


The George Washington University Hospital

Information Access Management to support clinical Research

Protocol Specification

Effective - January 1, 2012



December 14, 2011

Introduction

The George Washington University Hospital's Information Security & Privacy compliance committee has developed this protocol that facilitates the education and adoption of an improved information access process for current and future research projects underway at the hospital.

The process outlined in this proposal, serves as a general guideline to estimate time frames, required documentation as well as controls that need to be in place in order to ensure proper privacy and security of ePHI that will be needed to support the research activities.

Scope

The audience of this document includes but is not limited to:

1. Hospital Administration
2. University Administration responsible for clinical research
3. Principle investigators / Researchers
4. Hospital IT

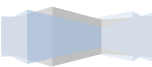
Documentation

The Information Security & Privacy Compliance committee at the hospital has outlined the following process in order to improve the time required to review the application.

Please Note: At this time, the following documentation is only required for Investigator led research projects. **For sponsored projects, please contact the Hospital Privacy/Security officer first, before submitting your documentation for approval.**

REQUIRED documentation to be considered for review

- a. IRB approval document
- b. HIPAA Full/Partial waiver as applicable, requiring GWUH privacy (and security officer if applicable) signature(s) to start research
- c. Research Protocol Synopsis
- d. Research Protocol
- e. In case only limited data sets/de-identified PHI is used for studies that are multi-agency and multi-location based
 - i. Copy of Data Use agreement (or similar) needs to be submitted if that data is going to be shared with others outside researchers/entity
- f. In case limited data sets/de-identified PHI cannot be used, provide documentation that specifies the following:



December 14, 2011

- i. Location where PHI will be stored. (Specify who owns the computers where ePHI will be stored)
- ii. Contact information for the Information technology resources responsible to maintain security on computers where ePHI is stored
- iii. Methods to restrict access and protect data backups
- iv. Date or time interval after which ePHI will be destroyed
- v. Evidence of HIPAA security and privacy training for staff that will have access to identifiable ePHI/hospital information systems
- vi. Start and End dates for individual access to hospital IT systems
- g. Except for GWUH credentialed physicians, please provide position descriptions pertaining to research, of MFA employees that will be working ONSITE at the hospital. Proof of credentials need to be provided in case of clinical care.
 - i. In case research staff includes staff that are 3rd party employees not affiliated with the MFA, please contact the Privacy/Security officer of GWUH for further guidance.
- h. Information System Access Request Form if needed
- i. All documents and forms NEED to have appropriate physical or electronic signatures prior to submission for review.

Processing Time Frames:

- a. Submission for Review:
 - i. At the current time, processing time frame for **hospital decision** is **at most 10 – 15 business days.**
 - 1. During review if the application is missing required information, the application will be sent back to the PI/IRB for update.
- b. There may be communications sent out to the PI for additional information. In this case, response is requested with 5 business days in order to avoid delays in processing of the application
- c. For applications that are sent for “pre-review” (i.e. parallel submission for initial feedback with the IRB), time line for review is the same as stated above.

Submission of Documentation

All application and supporting documents need to be sent to the following address:

Sumit Sehgal
Director, Information Security
Information Technology
The George Washington University Hospital
900 23rd Street N.W.
Washington, D.C 20037



December 14, 2011

Review Process

Once the application is received the following detailed reviews are performed during the 10 - 15 business days time frame.

1. Completeness of Information
2. Subject Selection / Screening Criteria and process impact on operations/patient satisfaction
3. Data required from Hospital Information Systems
4. Staff requiring access to Hospital Information Systems
5. Appropriateness of access
6. Security and privacy of **identifiable** ePHI if applicable
7. Data backup process
8. Data scrubbing and removal process
9. Hospital HR approval
10. Privacy officer review and approval

Upon completion of the required steps, the PI will be notified by email of approval following which they need to contact Hospital HR for scheduling the following tests for **any MFA employees (credentialed physicians are exempt from this requirement) that will be onsite for research:**

1. Criminal Background check and Physical (required by DC Law)
2. Drug Screen (Required by UHS policy)

The requirements above have been developed in collaboration with both the Hospital and MFA HR departments.

Parallel to this process, the PI will be provided a GWUH IT ticket # assigned to issue access to Hospital IT systems. Hospital IT will need proof of completion from HR before login information will be issued to research staff.

Audits

The Hospital Information Security and privacy staff have the authority to ask for (written request) proof of security measures specified in the proposal to prove effectiveness of controls. In the event of completion/expiration of a study, the PI may be asked to produce evidence of destruction of data as stated in the proposal.

Every occurrence of a reported or identified (in an audit) security or privacy incident will be investigated. The access of parties during that time shall be disabled during the assessment of facts and analysis.



December 14, 2011

Contact Information

For questions or concerns please contact:

Sumit Sehgal

Director, Information Security

Security/Privacy Officer

202-715-4511

Sumit.Sehgal@gwu-hospital.com

Supporting Documentation:

1. Information System Access Request Form
2. Consent to Drug Screen and background Check Form
3. Information Security Agreement





Information Security and Privacy Agreement

Universal Health Services Facilities and other UHS subsidiaries (collectively, “UHS” or “UHS companies”) are committed to maintaining high standards of confidentiality. The responsibility to preserve the confidentiality of information in any form (electronic, verbal, or written) rests with each User granted access to UHS information systems who may have access to Confidential Information, including Protected Health Information (PHI), Electronic Protected Health Information (ePHI), employee information, physician information, vendor information, medical, financial, or other business-related or company confidential information. Any information created, stored or processed on UHS systems, or systems maintained on UHS’ behalf by a vendor or other individual or entity, is the property of UHS, as is any information created by or on behalf of UHS, whether written, oral or electronic. UHS reserves the right to monitor and/or inspect all systems that store or transmit UHS data, the data stored therein, as well as all documents created by or on behalf of UHS.

Definitions:

Agreement means this *UHS Information Security and Privacy Agreement*.

Confidential Information means confidential information that is created, maintained, transmitted or received by UHS and includes, but is not limited to, Protected Health Information (“PHI”), Electronic Protected Health Information (“ePHI”), other patient information, Workforce member information, employee, physician, medical, financial and other business-related or company private information in any form (e.g., electronic, verbal, imaged or written).

Protected Health Information (“PHI”) means individually identifiable health information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. PHI can be oral, written, electronic, or recorded in any other form.

Electronic Protected Health Information (“ePHI”) means Protected Health Information in electronic form.

User means a person or entity with authorized access to any UHS network and/or other information systems, including computer systems.

Workforce means employees, volunteers, trainees, and persons whose conduct, in the performance of work for UHS, are under the direct control of UHS, whether or not they are paid by UHS. Workforce also include management and employed medical staff.

I HAVE READ AND UNDERSTAND THIS ENTIRE AGREEMENT, AND I AGREE TO THE FOLLOWING:

<i>(Note: Please initial each line in the space provided after reading it.)</i>	<u>Initials:</u>
1. I understand it is my personal responsibility to read, understand and comply with all applicable UHS company policies and procedures, including Security policies. I understand that these policies provide important information about the acceptable use of information systems, protection from malicious software, Mobile device usage, and data encryption, and other important information. If I am provided access to PHI or ePHI, I also	

agree to comply with the Privacy policies.	
2. I have been provided access to the Security (and Privacy policies as applicable).	
3. I agree not to disclose any PHI, ePHI or any other Confidential Information obtained by accessing the UHS network and/or other information systems, including computer systems, or otherwise to any unauthorized party. I agree not to access or use any PHI, ePHI or any other Confidential Information unless I am authorized to do so. I agree that all patient-related information shall be held to the highest level of confidentiality.	
4. I agree to access the UHS network and/or other information systems, including computer systems, only for purposes related to the scope of the access granted to me.	
5. I understand that UHS regularly audits access to information systems and the data contained in these systems. I agree to cooperate with UHS regarding these audits or other inspections of data and equipment, including UHS inquiries that arise as a result of such audits.	
6. I agree that I will not share or disclose User IDs, passwords or other methods that allow access to UHS network and/or other information systems, including computer systems, to anyone, at any time, nor will I share my account(s). I also agree to store all UHS company-related data onto the system servers rather than on hard drives of individual workstations, personal computers or other devices.	
7. I agree to contact my supervisor (or for non-employees, the applicable UHS Department Director or Business Contact) and IS Security Officer immediately if I have knowledge that any password is inappropriately revealed or any inappropriate data access or access to Confidential Information has occurred.	
8. I understand that Confidential Information includes, but is not limited to PHI, ePHI, other patient information, employee, physician, medical, financial and all other business-related or company private information (electronic, verbal or written).	
9. I agree that I will not install or use software that is not licensed by UHS (or that is otherwise unlawful to use) on any UHS information systems, equipment, devices or networks. I understand that unauthorized software may pose security risks and will be removed by UHS.	
10. I agree to report any and all activity that is contrary to this Agreement or the UHS Security or Privacy policies to my supervisor, Department Director, IS Security Officer or Privacy Officer.	
11. I understand that for employees this form will be part of the employee file at UHS and that failure to comply with this Agreement and the UHS Security and Privacy policies may result in formal disciplinary action, up to and including termination. I understand that for non-employees, failure to comply with this Agreement and the UHS Security and Privacy policies may result in revocation of access and the termination of any agreements or relationships with UHS.	
12. I understand that all information and/or data transmitted by or through or stored on any UHS device, or system maintained on any UHS company's behalf by a vendor or other individual or entity, will be accessible by UHS and considered the property of UHS, subject to applicable law. I understand this includes, without limitation, any personal, non-work related information. I do not have any expectation of privacy with regard to information on any UHS network and/or other information systems, including computer systems, and understand that UHS has no obligation to maintain the privacy and security of	

CONSENT TO DRUG SCREEN AND BACKGROUND CHECK

George Washington University Hospital (“GWUH”) conducts thorough reference and background checks of all applicants for employment, as well as for all independent contractors, volunteers, or other persons who provide patient care. Any individual who provides misleading, erroneous, or willfully deceptive information to the Company is immediately eliminated from further consideration for employment or services.

In connection with contract for services with GWUH, I understand that investigative background inquiries are to be made on me which may include consumer, criminal, driving, and other reports. These reports may include information as to my general reputation, character, mode of living, work habits, performance and experience. Further, I understand that GWUH may be requesting information from various federal, state and other agencies which maintain public and non-public records concerning my past activities relating to my driving, civil, education and other experiences.

I understand that if a background check discloses any misrepresentation or other information indicating that I am not suited to perform services for the Company, my services may be immediately terminated at the Company’s discretion.

I understand that this form will remain in effect for the duration of my contract with the Company.

Under the terms of the Fair Credit Reporting Act, I am entitled to know if employment is denied because of information obtained from a consumer-reporting agency. If so, I will be so advised and given the name of the agency or source of information.

All background results are considered confidential and will be disclosed within the Company only on a need to know basis and as allowed or required by law.

I also hereby give my consent and express my willingness to undergo a drug screen as requested by GWUH. Such request may be made by GWUH at any time during the duration of my contract. I also consent to the release of the results of the drug screen to GWUH. With this agreement, I am also consenting to the collection of any urine sample collected from me by GWUH’s designated physician or testing representative. I understand that if such a sample is collected, it is sent to a laboratory selected by GWUH, which conducts screening tests on it to detect the presence of illegal narcotics, including marijuana and other drugs, as well as signs of abuse of legal drugs. I consent to the release to GWUH of all of my medical records related to this physical examination and any drug test that contains relevant information about my fitness and ability to perform the functions of the work for which I would be performing for GWUH.

In exchange for GWUH’S scheduling and paying for these medical examinations and tests, I release and discharge GWUH and any of its designated medical personnel, agents, or authorized testing laboratories from any claims or potential liability arising out of or related to any physical or medical examination or the results of such examinations or tests. I also agree not to file or pursue any complaints, claims, or legal actions of any kind against GWUH or any of its employees, representatives, or agents arising out of their activities or actions performed in connection with these physical or medical examinations.

(Signed) _____ Date _____

October 19, 2011

The George Washington University Hospital

Clinical Research – Network Access Form

Date: _____

Name: _____ / Title: _____

Employer: GW Hospital / MFA / OTHER: _____

Phone: _____

Email: _____

Study PI: _____ / Email: _____

Approved IRB# _____ / Date Approved: _____ / Expiration Date: _____

Signature of Requestor: _____ ; **Signature of PI:** _____

What data is required?

Clone Access (make access same as this research staff member): _____

What date will access need to be terminated? _____

FOR HOSPITAL USE ONLY:

Date of Hospital Approval: _____ / HR Processes Completion / Badge ID: _____

Access Approved by: _____ / Title: _____ / Date: _____

System Access Approved: