

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS006
	PFS Policies and Procedures Manual	<i>Effective Date</i>	03-17-00
	<i>Subject</i>	<i>Page</i>	1 of 1
	HDM Installation Request	<i>Revised</i>	08/01/05

POLICY

This policy applies to the Johns Hopkins Health System (JHHS) Patient Financial Services (PFS) Department.

PURPOSE

The purpose of this policy is to establish the proper procedure for obtaining access to HDM.

PROCEDURES

To obtain access to HDM, a service request must be submitted to JHMCIS to have the HDM software installed and the following forms must be completed.

- 1) Service Request:** submit request to Karen Preston at 4-3750 and have the words "HDM Software Installation" on the request, or fill out an on-line request at <http://itsr.jhmi.edu>
- 2) Read the CIMD Policy and Procedures:** Security and Access to Patient and Institutional Information at <http://datamart1.jhmi.edu/security.htm#top>
- 3) Complete the HDM User Information Sheet (Exhibit 1) and the Data Use Agreement (Exhibit 2):** Fax the forms to Damon Brooks at 0-9626.

Once approval has been granted, you will receive a log-in and password.

SPONSOR

Senior Director, Patient Financial Services, JHHS

REVIEW CYCLE

Three (3) years

APPROVAL

Senior Director, JHHS

Date

Exhibit 1

JHH Casemix Information Management & JHM DataMart

HDM User Information Sheet

Printed Name	Date	JHED ID	
--------------	------	---------	--

E-Mail Address	Title	Phone	Fax
----------------	-------	-------	-----

Johns Hopkins Entity (JHH, BMC, JHU, etc.)	Department/Division	Office Address	
--	---------------------	----------------	--

Computer Location	Computer Operating System (Windows 95, Windows NT, etc.)		
-------------------	--	--	--

If replacing a former employee, write name above

Data Use Justification

1. What information needs require you to access the requested data set(s)?

2. What type of analyses and reports will be generated from the requested data set(s)?

3. Who will receive the analyses and reports?

4. What security measures are in place to maintain the confidentiality of this data? Users should maintain password protection at machine power-on, workgroup login, screen saver (After 10 minutes of inactivity), and shared workstation directories. Physical security of any assigned workstation (including laptops) includes locking doors to rooms with workstations when absent for extended period of time.

5. I have read and agree to abide by the procedures in the CIMD Policy and Procedures: Security & Access to Patient and Institutional Information. (Available on CIMD Web site at <http://datamart1/security.htm>)

User Signature: _____

**Permission to access data will NOT be granted if this page is incomplete.
Fax to Damon Brooks at 410-550-9626 & call him at 410-550-9616 to confirm receipt.**

Exhibit 2

Johns Hopkins Hospital Casemix Information Management Department Data Use Agreement for *Confidential JHH HDM Clinical Monitoring System Data Set*

1. Electronic health information is an extension of the original health record, and shall be protected with the same diligence as the original medical record. The HDM databases contain health information identifiable by patient and provider, and therefore must be protected.
2. Only authorized personnel are permitted computer access to these databases. Access to the computer files is controlled through security codes (logons) and passwords known only to authorized users.
3. Authorization to the HDM databases can only be gained through a written request to the Director, Casemix Information Management Department (CIMD) or to the CIMD Security Coordinator.
4. Any request for diskette, tape or any other electronic form of this information that contains patient and/or provider specific data requires authorization as specified in section 3 above.
5. All reports based on these data indicate that the source of the data is Johns Hopkins Hospital HDM data.
6. CIMD staff reserve the right to inspect the offices of the data user to ensure compliance with this data use agreement.

My signature indicates that I have read, understand, and agree to comply with the data use requirements stated above. I understand that in the performance of my duties as an employee or contractor/consultant of Johns Hopkins Medicine and its affiliated entities, I must hold all patient medical information in confidence. I understand that any violation of confidentiality of medical information may result in punitive action in accordance with Johns Hopkins Medicine personnel policies.

Signature

Date

Printed Name

Access approved by: _____ on _____
JHH CIMD Date

Fax to Damon Brooks at 410-550-9626 & call him at 410-550-9616 to confirm receipt.