SECURITY AND PRIVACY OF PROTECTED HEALTH INFORMATION

(CREATED 12/02)

Rationale: Hudson Valley Community College recognizes a duty to avoid wrongful disclosure of Protected Health Information (PHI) of students, staff, faculty and others. It is a requirement of the College that every effort be made to protect the medical privacy of persons who have PHI on file with the College. This is done by protecting paper and electronic records as well as other health information through physical, administrative and technological means directed at maintaining the integrity and security of those records.

Goal: Secure and Protected Health Information

Objectives:

Training:

1. To maintain a training schedule for Health Science students to meet the requirements of affiliated institutions

2. To maintain an annual security and privacy training schedule for appropriate staff.

3. To update training modules as required.

Privacy and Security:

1. To maintain a secure environment wherever PHI is located, including areas of use and storage of medical and other health records.

2. To ensure staff behavior will uphold the privacy and security of PHI.

3. To maintain continuing review of security and privacy processes within the College and to develop or amend policies and procedures when necessary to protect PHI.

4. To maintain a program which allows for the transfer of Individually Identifiable Health Information upon written request of the individual and the revocation of that request as well.

5. To inform individuals submitting PHI of their privacy rights and to maintain a process to allow for satisfaction of complaints concerning the privacy and security of PHI.

6. To maintain accurate reporting, investigation and review of violations of security or privacy policy and determine sanctions for such violations.

7. To support a program which allows for amendments to medical and other health records.

8. To maintain an accurate accounting of disclosures of PHI.

9. To document all aspects of the security and privacy program.

Guidance for Disclosure of Protected Health Information

General Guidelines:

Generally, every disclosure must be evaluated on an individual basis. Identity of a requester of PHI must be appropriately verified.

Discussion for medical treatment, insurance processing and other normal business operations is allowed. Incidental observations are not appropriate.

Sharing identifiable information with the risk manager in case of possible liability, conversations with Human Resources Director or his/her Designee regarding ability of an employee to perform assigned duties, discussion of immunization information with Health Science Department Chairs and affiliating hospitals are examples of allowed communication because they fall under necessary disclosure for normal business operations. The Privacy Officer will advise staff with questions concerning disclosures of a questionable nature.

Policies:

Policy, Maintaining Physical Security of the PHI
The physical security of medical and other records containing Individually Identifiable Health Information will be maintained at all times.

Procedures:

Records containing PHI will not be left unattended in any place accessible to non-medical people.

Areas of location of Individually Identifiable Health Information must be locked at all times when staff members are not present in the immediate area to protect the security of PHI. Keys to such areas should be available only to those who need access to the health information.

At the end of each working day, all records containing PHI will be put in secure locked areas.

Records containing PHI will not be removed from their assigned location without permission of the Privacy Officer.

Policy, Staff Practices:
Staff will discuss or release PHI only for the purposes of treatment, insurance processing or when necessary to maintain normal business operations of the college and will take measures to avoid accidental release of PHI by careless record handling or verbal indiscretions.

Violators of any privacy policies will be subject to disciplinary action that ranges from reprimand to termination.

Procedures:

- Oral disclosures of information will be made only in emergency situations and then written or witnessed verbal consent of the concerned individual must be obtained if possible.
- Staff will never discuss an individual's PHI with another staff member within hearing distance of others.
- Staff will ensure identity of persons requesting PHI. SUNY card, Drivers License or other picture ID is acceptable identification.
- When speaking to someone concerning their health information, doors to an interview area should be closed. A TV, radio, CD or tape player should be used as sound for masking during interviews as well.
- Records containing PHI will not be left unattended and never be left where anyone other than appropriate staff can see or touch them.

Policy, College PHI Security and Privacy Committee:
A College PHI Security and Privacy Committee will be responsible for the security and privacy policies, procedures and protocols. **This does not abrogate the responsibility of individual employees to be vigilant with respect to any circumstances that may facilitate a breach of the security and privacy system.**

- The College PHI Security and Privacy Committee comprised of representatives from Health Services, Health Sciences, Human Resources, Finance, and Computer Services and FSA will review the security and privacy plan annually or more often if a need for policy change becomes apparent or applicable changes to the law occur. The Committee will make recommendations for change to the policy when necessary.

- Minutes of these meetings will be kept permanently.

- If the committee makes recommendations that are not approved by the relevant director or department chair, the recommendation must be reviewed by the Privacy Officer and the appropriate Vice President the ultimate decision concerning enactment of the recommendations will be made by the appropriate Vice President.
- In keeping with other Health Service policy, all changes to policy will be documented as revisions to the original policy and previous policies will be maintained for a minimum of 10 years.

Policy, Staff Training:
All Staff who may come in contact with PHI while performing their duties will be trained annually regarding HIPAA and HVCC policies and procedures of security and privacy.

Procedure:

- In general training will be conducted as a web based activity. Training will be developed the Privacy Officer or others as assigned.

- Any changes in policies or procedures will be disseminated and explained to staff immediately. The training module will be updated immediately upon change.

- In keeping with other College policy, training in which each individual staff member participates will be recorded in the Office of Human Resource Development.

Policy, Release of Medical Information: (See Faxing Policy)
All written requests for release of health or medical information will be reviewed and the minimum information necessary to meet the purposes of the request will be released.

Research involving access to any individually identifiable student health information is prohibited.

Medical information will be released only upon written permission of the patient, a judicial subpoena or other legal requirements. **This includes all information released to another medical office.** Information regarding medical history or treatment will not be shared with faculty or administration unless the patient has requested such in writing (verbal permission is acceptable in extreme emergency but must be given in presence of witness). **The exception to this is that accident reports will be faxed to the College Risk Manager immediately upon completion.**

Procedure:

- Subpoenas and other legal forms will be evaluated by the Privacy Officer and/or the College Attorney, if necessary, before honoring the legal request for transfer of records .

- A "Request for Disclosure" form should be completed by the patient or his/her legal representative.

- Request for Disclosure forms must contain the following information:

  Name, address, Social Security number, and relationship of person requesting transfer,

  Exact description of information to be transferred,

  Purpose of disclosure,

  Name, address and, if appropriate, fax number of where the records should be sent,

Signature of person requesting the transfer and date of signature,

Witnessing signature of transfer request.

- All requests for disclosure must be examined carefully and with the exception of a request for Immunization or Physical Exam information that is signed by the student or staff member, all requests will be reviewed by the Privacy Officer who will use discretion in referring these requests to the College Attorney.

- Information disclosed will always be limited to the exact information authorized.

- Written permission must be signed by the student/ patient unless that person is under the legal age of consent, in which case the legal guardian should sign the letter/form. Proof of legal guardianship will be approved by the College Attorney.

- If a Request for Disclosure form or a letter of request is signed by someone claiming to be a legal representative, the request must be approved by the Privacy Officer or the College Attorney. The documentation of representation must be attached to the form.

- The letter/form must specifically address what information is to be released and cannot be used for more than one transfer of information.

- When the "Request for Disclosure" Form is completed the information will be photocopied and mailed to the address indicated or given to the individual requesting his/her records.

- The request will be retained with the Health information released and in the Disclosure Log. A note that the copy was faxed and mailed or given to the individual and the date will be noted on the request and, if appropriate, on the Clinical notes of the patient's record.

- ONLY FORMS ORIGINATING AT HVCC OR AT THE REQUEST OF HVCC CAN BE COPIED AND SHARED WITH OTHERS. FORMS GENERATED AT OTHER PLACES CANNOT BE TRANSFERRED.

Faxing of PHI:

Faxing of Protected Health Information will be done only after a request by the subject of the PHI.

Procedure:

- Numbers to which information will be faxed may be accepted if given by the subject of the PHI.

- Numbers which are researched by college staff must be verified by calling the office to which the information is to be faxed.

- A cover sheet must accompany the information and the cover sheet must have the standard information:

1. Name, telephone and fax number of the person the PHI is being faxed to,
2. Name, address and telephone number of the person from whom the PHI is being faxed, Date the fax is being initiated,
3. Number of pages being faxed, including cover page,
4. Subject or topic of the fax.
5. The cover sheet should also contain a confidentiality notice. The statement should include:

CONFIDENTIALITY NOTICE

THE INFORMATION ACCOMPANYING THIS FACSIMILE COVER SHEET CONTAINS PRIVILEGED AND CONFIDENTIAL INFORMATION INTENDED SOLELY FOR THE USE OF THE INDIVIDIUAL OR ENTITY TO WHOM IT IS ADDRESSED. IF THE READER OF THIS NOTICE IS NOT THE INTENDED ADDRESSEE, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED.

IF YOU HAVE RECEIVED THIS FACSIMILE IN ERROR, PLEASE NOTIFY US BY TELEPHONE IMMEDIATELY AND EITHER RETURN THE FAXED INFORMATION TO THE SENDER, BY US MAIL, AT THE ADDRESS LISTED ON THIS FACSIMILE, OR DISPOSE OF THE DOCUMENT BY SHREDDING. THANK YOU

- After a fax transmission is completed, the fax the number on the transmittal form will be verified as the proper number to which the information should have been faxed. The transmittal form will then be attached to the cover sheet and a copy of the information that was faxed. These papers will be kept in the medical record with the original information.

Policy, Right to Revoke Authorization:
Each individual has a right to revoke an authorization previously signed by completing an "Authorization Revocation Form".

Procedure:

- After signing and witnessing of the "Authorization Revocation Form" a copy shall be given to:
  The patient requesting revocation
  The Privacy Officer
  A third will be filed with the health information
- The revocation will be entered in the revocation log.

Policy, Accounting of Disclosure of Protected Health Information:
A complete accounting of individual disclosures of protected health information will be maintained on each individual record and in a disclosure log. A separate record will be maintained by the Privacy Officer.

Procedure:

- Required information to maintain in the Disclosure Log for each disclosure is as follows:
  1. Date of disclosure
  2. Name and address of person to receive the disclosed information
  3. Description of disclosed information
  4. Statement of purpose of disclosure
  5. Written accounting of disclosure will be provided to the individual
  6. Title of person who approved the disclosure
  7. The disclosure log will be archived annually.

Policy, Right to Request Restriction of Use and Disclosure of Protected Health Information:
A person requesting restriction of use or disclosure of his/her protected health information should be informed that the College may be unable to restrict disclosure. Other restriction requests will be processed by the Privacy Officer.

Procedure:

- Upon request for restriction of use or disclosure, the individual will be given a request for restriction form.

- The Privacy Officer will process the request with in 10 working days. During that time no PHI will be disclosed.

- If the request is denied, the requestor may appeal to the appropriate Vice President by completing an appeal form. The Vice President will notify the individual of the decision within 10 days.

- Upon approval of a "Request of Restriction of Use and Disclosure Form", a copy will be placed with the student's health information and a "Restriction" stamp will be applied on the outside of the folder. If put in storage without a file jacket, the file will have a red "Restricted" sticker put on the front page of the health information.

Policy, Notice of Privacy Practice:
Every effort will be made to inform students and employees of the College Privacy Practice.

Procedure:

A copy of the Notice of Privacy Practice will be placed in the College Catalog, the Student Handbook and the Employee Orientation Packet.

Policy, Processing of Complaints Regarding Privacy Policies
Students have a right to have complaints heard and responded to in a timely manner.

Procedure:

- Upon request, the complainant will be given a Privacy Complaint Form to complete.

- The completed form will be sent to the Privacy Officer at once.

- All complaints regarding privacy policy will be processed by the Privacy Officer within 10 working days.

- Appeal of unsatisfied complaints will be sent to the Vice President of Student Services upon completion of an Appeals Form. Appeals Forms must be completed within 10 days of notification of the Privacy Officer's decision.

Policy, Investigations of Violations of Privacy Policy
All complaints of violations of privacy will be thoroughly investigated.

Procedure:

- Investigations of privacy violations will be directed by the Privacy Officer and completed within 10 working days of the complaint.
- A complete report of any investigation will be given to the Vice President of Student Services upon completion of the investigation.

Policy, Review and Amendment of protected Health Information:
Anyone wishing to review or amend his or her health information may apply to do so.

Procedure:

- Persons wishing to review or amend their health information must process a "Request for Review" or "Request for Amendment of Medical Record" form that will be processed by the Privacy Officer. These requests will be processed within 10 business days.

Review and Amendment Decision:
The applicant will be notified of the Privacy Officers" decision concerning the review/amendment request within 15 working days of the date of the original request.

Procedure:

- If the review/amendment is approved the Privacy Officer will direct the involved administrator to place the amendment in the health information.

- If the review/amendment is denied, the Privacy Officer will explain to the applicant in writing reasons for denial within 15 days of the application. The Privacy Officer will also explain the process for appeal to the appropriate Vice President.
- The applicant may appeal a denial to the Vice President by filing an appeal form within 10 working days of the decision.
- The Vice President will notify the applicant of his/her decision within 10 working days of receiving the appeal.
- In the case of denial of the appeal, the Vice President will notify the complainant of his/her right to complain to US Health and Human Services.
- The Vice President may allow the involved administrator to file an opposing view of the amendment in the health record.