STUDENT PACKET

Please Return Completed Packet to:

Sharp HealthCare
8695 Spectrum Center Blvd.
San Diego, California 92123
ATTN: SRN/Affiliation – Claudia Bock

NOTE:

Please do not include your health record documentation with this packet.

Student Packet

Check List

Return the following Completed Forms to:

Sharp HealthCare
8695 Spectrum Center Blvd.
San Diego, California 92123
ATTN: SRN/Affiliation-Claudia Bock
Fax 858-499-5327

- *[ ] Placement Request Form*
- *[ ] Declination: Hepatitis B Vaccine (if applicable)*
- *[ ] Proposed Publication Approval Request*
- *[ ] Delegated Faculty Member*
- *[ ] Training Verification Form*
- *[ ] Signed Confidentiality and Non-disclosure Agreement*

- User ID and passwords to Sharp computer applications will be issued upon receipt of the above documents.
- School should maintain copies of post-tests and exams in student file.
- Do not include health record documentation with this packet.

PLACEMENT #:

SHARP
HEALTHCARE

PLACEMENT REQUEST FORM DATE:

SCHOOL NAME:	
STUDENT'S NAME:	**STUDENT'S PHONE #:**
INSTRUCTOR:	**INSTRUCTOR'S PHONE #:**
PROGRAM	**COURSE #:**
ROTATION WILL START:	**ROTATION WILL END:**
THE TOTAL NUMBER OF HOURS STUDENT NEEDS IS:	**WHAT SHIFT:**
DAYS AVAILABLE:	**PRECEPTOR'S NAME (if known):**
WHAT FACILITY :	**HAS PLACEMENT BEEN APPROVED BY THE SITE?** **If so, who approved:** **PHONE NUMBER:**

MANDATORY: (All Students and Instructors): Sharp HealthCare training modules for HIPAA, Corporate Integrity and Information Security must be completed before starting clinical rotation/internship. .

INSURANCE INFORMATION: (For clinical students) - A certificate of Professional Liability must be attached or on file at Sharp's SRN/Affiliation office – see address below.

HEALTH SCREENING: (All students) It is the student's responsibility to meet health screening requirements prior to beginning their rotation.

The following is a check off list showing the items students need to be in compliance with before starting their rotation. REMINDER: Please DO NOT SEND health records – just check off the items on the list you are in compliance with. Thank you.
(ALL STUDENTS and INSTRUCTORS on site with students)

_____Annual tuberculosis screening: Mantoux tuberculosis test or if positive Health Departments guidelines for follow up.
_____ Positive titer to rubella and rubeola or vaccination against same or a physician's statement of disease concerning rubella and rubeola
_____ Varicella immunity
_____Immunizations: Tetanus
_____CPR – Will be required if the area the student is in requires it
_____Vaccine/immunity Hepatitis B or signed declination form

RETURN PACKET TO: Sharp HealthCare, 8695 Spectrum Center Blvd, San Diego, CA 92123, Attn: SRN/Affiliation.

f:/word/my doc/Affiliation/CPRF
revised 02-01-05

SHARP
HEALTHCARE

DECLINATION: HEPATITIS B VACCINE

I understand that I may be exposed to blood or other potentially infectious materials and be at risk of acquiring hepatitis B virus (HBV) infection. I decline hepatitis B vaccination at this time. I understand that by declining this vaccine, I continue to be at risk of acquiring hepatitis B, a serious disease.

NAME:_____ **DATE:** _____
(please print)

SIGNATURE: _____

SCHOOL: _____

PROGRAM: _____

SHARP
HEALTHCARE

AFFILIATION AGREEMENT

ATTACHMENT C

PROPOSED PUBLICATION APPROVAL REQUEST

I agree that all proposed publications written by me, based on information/data/business experience obtained at the FACILITY, will be submitted to the FACILITY for its written approval prior to being submitted for publication.

DATE:_____

STUDENT SIGNATURE_____

STUDENT NAME (please print):_____

SCHOOL'S NAME_____

SHARP

HEALTH TRAINEE

Required Training Verification

Name:_____
(Print Clearly)

School:_____

Program:_____

Type of Student: _____ **Instructor:**_____

I have received, read and understand the following modules*:

[] HIPAA Privacy Training Basics
[] Corporate Compliance
[] Information Security

_____ _____
Signature **Date**

_____ _____
School Representative **Date**

_____ _____
Signature **Title**

Send completed forms to:
Sharp HealthCare
Clinical Affiliation
8695 Spectrum Center Blvd
San Diego, CA 92123
Fax: 858-499-5237

*School should keep copies of post-tests in student file

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Obligations Regarding Confidentiality

Applies to all employees (including administration, managers, supervisors and applicable physicians); volunteers; agency, temporary and registry personnel; students, interns, and contracted personnel.

Patient health and Sharp Organizational information is protected by law and by Sharp HealthCare policies. The intent of these laws and policies is to assure that confidentiality of information is maintained while used for business and clinical operations. In my job, I may see or hear confidential information in any form (oral, written, electronic) regarding:

- Patients and/or their family members (such as patient records, test results, conversations, financial information)
- Employees, physicians, volunteers and contractors (such as employment records, corrective action, disciplinary action)

I AGREE TO AND ACKNOWLEDGE THE FOLLOWIN G:

- I will protect the privacy of all business and medical information relating to our patients, members, employees and health care providers.
- I know that confidential information I learn on my job does not belong to me and I have no right or ownership to it. Sharp HealthCare may take away my access to confidential information at any time.
- I will not misuse confidential information and will only access information necessary to do my job. I will not disclose any confidential information unless required to do so in the official capacity of my relationship, employment or contract with Sharp HealthCare.
- I will not share, change or destroy any confidential information unless it is part of my job to do so. If any of these tasks are part of my job, I will follow the correct department procedure or the instructions of my supervisor (such as shredding confidential paper). If a demand from an oversight agency, law enforcement or government agency is made upon me from outside Sharp HealthCare to disclose confidential information, I will document this by giving written notice to my supervisor.
- I will only print information from a Sharp HealthCare information system when necessary for a legitimate work related purpose. I am accountable for this information until it is properly filed or disposed of.
- If I have access to electronic equipment and/or records, I will keep my computer password secret and I will not share it with any unauthorized individual. I am responsible to protect my password or other access to confidential information. I understand that my use of an electronic system may be periodically monitored and audited to ensure compliance with this agreement.
- I understand that I have an obligation to report to my supervisor and/or the Compliance Hotline if I think someone is misusing confidential information or is using my password. I further understand that Sharp HealthCare will not tolerate any retaliation against me for making a report.
- On termination of my employment, I will return to Sharp HealthCare all copies of documents containing Sharp HealthCare's confidential information or data in my possession or control.

I understand that failure to comply with this agreement may result in corrective action up to, and including, termination of employment or other relationships with Sharp HealthCare. I understand that I may also be subject to other remedies allowed by law. I understand that I must also comply with any laws, regulations, and Sharp HealthCare policies, including the Commitment to Principles, Privacy, Confidentiality and Security policies that address confidentiality. This agreement shall survive the termination of my official relationship, employment or contract with Sharp HealthCare.

I have read and understand this Confidentiality and Non-Disclosure Agreement, have had my questions fully addressed and have received a copy.

Date:_____ _____

Printed Name Signature

Date:_____ _____

Printed Name Witness

HIPAA Privacy Basics

Components

1. 8 pages reading material
2. 1 page post test

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #1

Title: **Confidentiality of Protected Health Information (PHI)**

SUMMARY

This policy describes the legal and ethical responsibility for the protection of privacy and confidentially of patients protected health information (PHI). The policy establishes responsibilities and safeguards that all personnel are responsible and accountable for following. In addition, sanctions for the misuse and inappropriate access of protected health information are described in the policy. The expectation to protect health information applies to everybody that has access to the healthcare environment, whether an employee, physician, volunteer, student, intern or contractor. Your signature on the Confidentiality and Non Disclosure Agreement establishes your commitment and obligation to the protection of information.

CRITICAL EDUCATION POINTS

Our Responsibilities

- To protect the health information that identifies a patient, is created in the process of caring for the patient, and is kept, filed, used or shared in an oral, written or electronic format.
- Determine and apply appropriate safeguards for protection of information in consideration of patient care needs and safety.
- Report suspected violations of privacy and confidentiality

Minimum Necessary, Need to Know: Only access information needed to do your job. You are **not** allowed to view or obtain information about you, your co-workers, family, or friends.

Unauthorized Access: Accessing or communicating confidential information not associated with your job responsibility is considered a violation of this policy and will result in corrective action which may include termination of your relationship with the organization, and also have personal legal consequences.

Apply Standard Safeguards

- ✓ Know the additional privacy practices and policies specific to your department.
- ✓ Protect confidential information from unauthorized access, use or disclosure.
- ✓ Maintain physical security, access control, locked storage as appropriate, i.e., keep doors closed to secure areas, obey posted signs for restricted access to secure areas).
- ✓ Notify a clinical staff member if medical records are left unattended in public view.
- ✓ Never dispose of paper or items containing patient information in the regular trash.
- ✓ Confidential information should never be discussed in public areas, such as hallways, cafeterias, or restrooms.
- ✓ Report known or suspected violations of privacy.
- ✓ Computer passwords are unique, do not share your password or log on a computer for someone else.
- ✓ Stop and question individuals who do not belong in your work area.
- ✓ Never remove paper or items containing patient information from the facility unless authorized to do so.

- ✓ **Reporting privacy concerns and suspected violations,** lead to improved practices and further fosters a culture of respect for our patient's. Each of us has an obligation to report suspected violations and concerns. There will be no retaliation for reports made in good faith. Report concerns to the charge nurse or your supervisor.

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #2

Title: **Provision of the Notice of Privacy Practices**

SUMMARY

Each hospital / facility will provide all patients accessing patient health services with a Notice of Privacy Practices. The Notice informs individuals of the permitted uses and disclosure that may be made of their health information, the individual's rights regarding his/her information and the organizations legal responsibilities with respect to protected health information. Privacy Regulations mandate elements that must be included in a notice. All personnel should read the Notice of Privacy Practices, know their responsibility for protecting information and be able to direct individuals who have questions or complaints regarding privacy practices to the appropriate resource.

CRITICAL EDUCATION POINTS

Right to a Notice of Privacy Practices (NPP)

The Notice of Privacy Practices serves to inform individuals or their legal representative of:

- ✓ Ways we may use and disclose their protected health information (PHI)
- ✓ Their rights regarding their health information
- ✓ Legal responsibilities with respect to PHI

- **Required Notice elements may be found in 45 CFR 164.520**

- **Notice must be provided at the time of "1st" service delivery**
  - ✓ Patients must be provided with the NPP at least once after 4/14/03, at the first service delivery
  - ✓ In emergency treatment, the notice must be provided as soon as reasonably practical
  - ✓ The notice may be furnished electronically, mailed or faxed if the patient authorizes
  - ✓ The Notice will be posted in service areas and on the Health care providers web site

- **Acknowledgement of Receipt of the Notice**
  - ✓ A good faith effort must be made to obtain written acknowledgement from the patient or their legal representative that they received the notice
  - ✓ If patient refuses to sign or is unavailable to sign (e.g. left before signature could be obtained), document efforts to obtain the signature
  - ✓ Signed acknowledgments are retained for 6 years according to each facility's procedures, e.g., EDI, SV3 for scanning

- **Inform Patients of the "Patient / Facility Directory"**
  - ✓ Patient Directory includes only name, location in facility, one-word condition description and to verified members of the clergy, religious affiliation.
  - ✓ Patients may restrict all or part of their information in the directory, usually at the time of inpatient admission.

- **Restriction of Information**
  If patients request restrictions on their information beyond inclusion in the Patient Directory, notify a supervisor to speak to the patient. Accommodating further restrictions to their information will be based on the scope of the request and each facility's system capabilities to provide restrictions.

- **Requests for alternate "confidential communications"**
  Patients may request that their information be communicated in alternate manner. An example may be that a patient requests that a bill be sent to an alternate address. Access / registration staff will accommodate reasonable requests.

- **Patient questions and concerns regarding our privacy practices**
  Refer patients to your supervisor or the Privacy Officer

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #3

Title: Information, Disclosure of Patient / Facility Directory to the Public and Media

SUMMARY

The privacy regulations allow the disclosure of certain information maintained in a "Patient / Facility Directory". The information contained in the directory is very limited. Patients are informed of the Patient Directory at each admission and have the opportunity to restrict entirely or limit information that may be disclosed. This policy provides guidance for the disclosure of Patient Directory information to family, friends, clergy and the media who ask for the patient by name.

CRITICAL EDUCATION POINTS

Patient Directory

The company will maintain a directory of individuals currently in the facility with specific information that may be released to the public, media, family, friends who inquire about the patient by name. **Exception,** for further protection of privacy, behavioral health and alcohol treatment patients will never be included in the Patient Directory.

At the time of admission or as soon as reasonably possible, patients will be asked if they want to be included in the Patient Directory. They may choose to include or restrict all or part of their information in the directory.

Directory Information is limited and may only be released to individuals who inquire about the patient by name, information includes:

- ✓ Patient name
- ✓ Location (e.g., Emergency Department or Inpatient)
- ✓ Condition (one word), obtain from physician or appropriate clinical staff
- ⇨ *Undetermined: Patient is awaiting the physician and assessment*
- ⇨ *Good: Vital signs are stable and within normal limits. Patient is conscious and comfortable. Indicators are excellent*
- ⇨ *Fair: Vital signs stable, within limits. Patient is conscious but may be uncomfortable. Indicators are favorable.*
- ⇨ *Serious: Vital signs may be unstable and not within normal limits. Patient is acutely ill, indicators are questionable.*
- ⇨ *Critical: vital signs are unstable and not within normal limits. Patient may be unconscious. Indicators are unfavorable.*
- ✓ Religion (available only to clergy)

Patient Restrictions: If a patient restricts their information, they are registered as "Confidential" and will not show up in the Patient Directory when an inquiry is made. Response for inquiries should be, " We do not show an individual by that name in our Patient Directory". If a caller is persistent, contact a supervisor for assistance.

Media Requests for Information:

- ✓ Media requests for information regarding a specific patient. Patient Directory information may be provided to the media if they inquire about the patient by name. If the media does not have the patient name, no information will be disclosed.
- ✓ Marketing and Communications or an Operation Supervisor should be called to respond to all media requests.
- ✓ Media should always be escorted while in the facility. Ask media members to wait in the lobby while you call your supervisor or communications representative for an escort.

EDUCATION AND DEVELOPMENT SUMMARY SHEET - # 4

Title: **Facsimile (Faxing) of Protected Health Information (PHI)**

SUMMARY

This policy provides staff with guidance on the appropriate use of facsimile (fax) transmission of information to ensure the confidentiality and security of information. Use of fax for communication of protected health information and the necessary safeguards to practice are addressed in this policy.

CRITICAL EDUCATION POINTS

Utilization of Fax transmission for communication of information will be determined using the following criteria:

- ✓ that fax transmission is the appropriate means of communication
- ✓ that sender's authority to disclose and the recipient's authority to receive information is verified
- ✓ that security status and protection requirements of information being transmitted is considered

Protected Health Information (PHI) may be transmitted by fax when:

- ✓ Original record or mail delivered copies will not meet the immediate needs of patient care
- ✓ When PHI is urgently required by a third party payor and failure to facsimile the records could result in loss of reimbursement
- ✓ Pursuant to a patient/legal representative's authorization

Authorization to Disclose PHI:

Assess the need for specific patient authorization to disclose the information prior to faxing.

Limit information being faxed to the minimum necessary:

Faxed information should always be limited to the amount necessary to achieve the purpose of the communication. Limit information to effectively facilitate safety, treatment, essential healthcare operations and continuity of care.

Fax Safeguards:

- Verify accuracy of fax numbers with intended recipient before sending a fax
- **Notify facilities that you commonly receive faxes from if your number changes**
- Recipients you commonly fax numbers to should be pre-programmed
- When faxing PHI, verify fax number and availability of recipient prior to sending
- Locate machines out of public view
- Establish a routine for regular removing/distribution of incoming faxes

Pre-programmed Fax Numbers:

- Use pre-programmed numbers whenever possible
- Pre-program number and send test fax-requesting verification of receipt

Fax Cover Sheet Requirements:

- Completed cover sheets with standard confidentiality statement and disclaimer are required on all organizational fax transmissions.

Exception: Routing faxing of information from department to department within the building, using a pre programmed fax number may not require a fax cover sheet. See policy for details of requirements.

Misdirected faxes:

- Obtain the fax number of the unintended receiver and immediately transmit a request that the material be destroyed immediately or retrieved by mail or delivery
- If fax contained PHI, notify a supervisor

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #5

Title: **Health Information: Access, Use and Disclosure of PHI**

SUMMARY

To ensure the protection and confidentiality of protected health information in compliance with state and federal regulations, this policy describes the circumstances under which you may access, use and disclose protected health information as well as the types of authorization required.

CRITICAL EDUCATION POINTS

Staff authorized to disclose protected health information (PHI) should be familiar with all facility policies regarding the authorization and disclosure of information. Policy highlights include:

Access to PHI: Access to PHI is limited to those individuals:

- ✓ Providing care and treatment
- ✓ Requiring information for payment/billing activities
- ✓ Participating in functions of health care operations

Use of PHI:

The Privacy Regulations allow use and disclosure of a patient's protected health information without a patient authorization in the following circumstances:

- **For providing Treatment, Payment and Health Care Operations (TPO):** In order to carry out treatment, payment and healthcare operations, i.e. sharing information with other providers, transfer of patient to another facility, coordinating continuing care. Payment activities with third parties for the purpose of obtaining payment. Risk management and utilization review and performance improvement activities in support of hospital operations.
- **Mandated and required reporting:** Staff will continue to disclose PHI as mandated or required under various state and federal regulations, i.e. abuse, assault, infectious disease, public health activities, organ and tissue donation.
- **Individuals Involved in the patients care:** Clinical staff may share relevant information with individuals who have been identified by the patient as being involved in their care.

HIV/AIDS test results, Psychiatric and Drug/Alcohol treatment Information always requires specific Patient Authorization for disclosure under all circumstances: These types of information are protected under additional regulations and must have patient authorization for release. The attending physician must be consulted prior to release of any mental/behavioral health information to a patient.

Disclosure of PHI: Generally any disclosure made outside of the organization, not for the purpose of TPO or mandated by laws, requires patient authorization. Always consider the circumstance information is being released under. If in doubt, consult with Health Information Department or obtain the patients authorization. Use the standard "Authorization for Use and Disclosure of Health Information" form found on all units and in the Health Information Department.

Responding to requests for information: Whenever possible, Health Information (HI) personnel should process requests for information. If HI is not available however, authorized personnel may disclose the information. It is critical that the policy and procedure is followed closely and the appropriate documentation form be completed and signed.

Verify Authority and Identity: When disclosing information, verify the authority of the individual requesting information, check identification by asking for ID or use call back.

Documentation of Disclosures: It is important that disclosures made outside of the organization for reasons other than TPO be documented. Complete the appropriate documentation form and ensure that it is included in the medical record or provided to the Health Information Department. This includes oral, written and electronic disclosures and disclosures made in error. Examples include, mandated and required reporting, verbal disclosures to law enforcement.

Patient Access: Patients have a right to view or obtain copies of their health information. Refer the patient to Health Information department whenever possible. There are circumstances when access to records may be denied. Clinicians responding to patient's requests for access to their information should be familiar with the circumstances in which access should be denied. For patients requesting to view their open medical record, a physician order is required. Have an appropriate clinician available to review the information with the patient.

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #6

Title: **Health Information: Disclosure of PHI to Law Enforcement**

SUMMARY

The Privacy Regulations allow the disclosure of certain protected health information to law enforcement officials without the authorization of the patient. This policy describes the circumstances under which information may be released to law enforcement and the elements of information that may be released.

CRITICAL EDUCATION POINTS

Generally, the disclosure of Protected Health Information (PHI) to law enforcement or under state/federal law without a patient authorization is limited to the following:

- ✓ To comply with legal processes (e.g., subpoena, court order, warrant, mandated and required reporting)
- ✓ To help identify or locate suspects / fugitives (on or off premises)
- ✓ To provide information about victims of a crime
- ✓ To report crime on the premises
- ✓ To correctional institutions

Refer to Health Information Department: Requests from law enforcement or for legal processes should be referred to the Health Information Department whenever possible. In emergency situations, clinical staff may disclose non-medical PHI.

Request identity and validate authority prior to disclosing information:
In all circumstances of disclosure, the requestor's identity and authority must be validated and documented.

- **State and Federal Mandated and Required Reporting.** California Law (CMIA) is not as broad as HIPAA. Disclosures of medical information to law enforcement is authorized pursuant to a court order, subpoena or search warrant, and/or if required by other laws. Examples include child abuse, domestic abuse, assault, neglect, subpoena, summons, and psychotherapy notes (with authorization from the note's originator). Health care providers are required to report certain types of wounds and physical injuries, such as gunshots, stabbing, and burns, subject to applicable laws. Reference specific policies for mandated and required reporting;

- **Disclosure of PHI to Law Enforcement for Suspected Felon. Location & Identification Information:** In response to an inquiry regarding a specific patient, in the absence of a subpoena, court order or warrant, California Law (CMIA) limits the disclosure to **non-medical information**, e.g., suspect's name, address, age, and sex; a general description of the patient's condition, treatment and the nature of the injury, burn, poisoning, or other condition. Note: Do not disclose PHI related to the individual's DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissues.

- **Disclosure of PHI to Law Enforcement for Victims of Crime.** In responding to an official request concerning a person who is suspected of being a victim of a crime, PHI may be released with the individual's authorization. Without an authorization, disclosure of PHI must be in the best interest of the individual in the professional judgment of the provider and limited to non-medical information. For decedent-victims: Report the suspicion that death involved criminal conduct.

- **Reporting Crime to Law Enforcement – Crime on the Premises.** PHI disclosure is limited to non-medical information, e.g., nature of crime, location of victim and/or suspected felon, identity, location and description of suspect.

- **Permitted Disclosures to Correctional Institution - No authorization required.** The company may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate, if the correctional institution / law enforcement official represents that the PHI is necessary for:
  a. The provision of health care to such individuals
  b. The health and safety of such individual, other inmates, or others at the correctional institution (e.g., officers, employees, persons responsible for transporting / transferring inmates)
  c. You may reasonably rely on the representation of such public officials for the authority to release PHI

Document disclosures: These types of disclosures must be documented in order to be included in an accounting of disclosures if requested by the patient. Documentation may be made on a required reporting form if available, i.e., assault, abuse required forms or may be documented on a "Report of PHI Disclosure Form" or other disclosure accounting system. Place copies of required reporting form or the Report of PHI Disclosure form in the medical record or forward to the Health Information Department.

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #7

Title: **Health Information: Request for Accounting of Disclosures of PHI**

SUMMARY

One of the new rights established in the Privacy Regulations is the patient's right to obtain an accounting of disclosures made of his/her health information. The accounting may include up to 6-year period, and generally includes disclosures that the patient may not be aware of that were made of their PHI, e.g., public health disclosures. This policy establishes procedures for how patients may obtain an accounting of disclosures as well as staff documentation procedures of disclosures that must be included in the accounting.

CRITICAL EDUCATION POINTS

- The Notice of Privacy Practices informs patients of their right to obtain an accounting of disclosures of their health information. Patients are informed that they must submit a request in writing to the Health Information Department.

- An accounting does not include all disclosures of a patient's PHI. Disclosures that are made for treatment, payment and health care operations or authorized by the patient are not included. Generally, disclosures required by law and regulations are included in the accounting. Examples of these types of disclosures include:
  - ✓ Disclosures required by law
  - ✓ Abuse, assault, domestic violence reporting
  - ✓ Judicial and administrative proceedings
  - ✓ Public health activities
  - ✓ Organ and tissue donation
  - ✓ Research purposes

Staff making disclosures in this category must document such disclosures and forward the information to Health Information for accounting purposes or document the disclosure in the on-line system, if available at the facility.

- Documentation may be done in one of three ways:
  1. Complete a "Report of PHI Disclosure". Include the form in the medical record or forward it to Health Information. The form may be used in circumstances such as verbal disclosures to law enforcement. Or when there is mandated reporting and standard reporting forms are unavailable.

  2. Copy of a standard reporting form is included in the medical record. Examples include, assault, abuse, neglect reporting. These forms are completed by the individual making the disclosure and are copied to the medical record.

  3. Maintaining a database of individuals whose information has been disclosed outside of the company. Examples include infection control reporting and lab reporting of infectious disease. Also included would be the IRB database of research protocols where patient information may have been viewed through a waived authorization.

- Elements of each disclosure required in the accounting are:
  - ✓ Date of disclosure
  - ✓ Name (and address if known) of the entity or person who received the PHI
  - ✓ Brief description describing the PHI disclosed
  - ✓ Brief statement describing the purpose of the disclosure of PHI (basis for the disclosure)

When Health Information receives a request for an accounting, they will review the entire medical record and available data base, i.e., infection control and IRB to compile a log of all disclosures required in the accounting. If you are unsure as to whether a disclosure is required to be accounted for, complete the Report of PHI Disclosure, the Health Information Department will determine on a case-by case basis whether the disclosure must be included in the accounting.

EDUCATION AND DEVELOPMENT SUMMARY SHEET - #8

Title: **Health Information: Request for an Amendment of PHI**

SUMMARY

Under current California regulations and the new Privacy Regulations, patients have the right to request an amendment to their health information if they believe their information is inaccurate or incorrect or incomplete. This policy establishes procedures for the patient request to amend their health information.

CRITICAL EDUCATION POINTS

Privacy regulations provide patients the right to request amendments to their protected health information (PHI). For example, a patient may ask to change an entry of incorrect, incomplete, or outdated information about them such as name, birth date, or admission date. Or, the patient may ask to amend medical, diagnostic, or treatment information such as progress notes and test results. They also may request the addition of a written addendum to their health information.

- The Notice of Privacy Practices provided during admission informs the patient of their right to submit a written request to amend their health information.
- Refer patients who desire to amend their health information to the Health Information Department. Patients may make a request during hospitalization or after discharge.
- Patients must submit their request to the Health Information Department, the request, must;
  - ✓ Be submitted in writing, (Health Information will provide a form)
  - ✓ Be limited to 250 words, or less, if it is a written addendum
  - ✓ Include a reason for the request
  - ✓ Identify others who need the amendment
- The Health Information (HI) Department must act on the request to amend a record within 60 days of receipt, or HI may obtain a one-time 30-day extension for responding to the patient's request provided that they meet the requirements necessary for the extension.
- Health Information, the physician, and/or Risk Management will review amendment requests as appropriate and determine:
  - ✓ The impact on the patient's care
  - ✓ Identity of any other entities that may rely on this amended information, and,
  - ✓ Provide a recommendation for agreement or denial of the amendment.
- If there is agreement for the amendment, Health Information will include the amendment in the patient's health record and if necessary make corrections.
  - ✓ Health Information will obtain authorization for the release of information to any other entity needing the amendment as identified by the patient or appropriate staff.
  - ✓ The amendment becomes a permanent part of the medical record and is included with any future third party disclosures. All communication of corrections, denials and rebuttals should also be included in future disclosures.
- If the amendment is denied, reason for denial will be documented. Examples of denials include:
  - ✓ PHI was not created by the organization
  - ✓ PHI is not part of the patient's medical record
  - ✓ Federal law forbids making the PHI in question available to the patient for inspection (e.g., psychotherapy notes)
  - ✓ PHI is accurate and complete as stated

Health Information Department will be responsible for providing a written notice to the patient and continued communication and correspondence as necessary.

HIPAA: INTERMEDIATE PRIVACY MODULE POST-TEST

DATE:_____

NAME:	TITLE:
SCHOOL:	LICENSE #:

Please circle the correct answer.

1. Staff may access and disclose only the amount of information necessary to achieve the purpose of the disclosure.
   TRUE FALSE

2. Patient or legal authorization is **always** required for the disclosure of the following types of information:
   a. HIV test results
   b. Alcohol and Drug treatment
   c. Psychiatric treatment
   d. All of the above

3. Patients may request an accounting of disclosures that have been made of their health information. Examples of disclosures required in the accounting include:
   a. Disclosures to law enforcement
   b. Mandated abuse, assault reporting
   c. Public health reporting
   d. All of the above

4. An authorization form from the patient is required to be completed when providing patients with copies of their health information.
   TRUE FALSE

5. A physician approval is required when patients request to view their open medical record.
   TRUE FALSE

6. When faxing information the following safeguards must be completed:
   a. Complete a fax cover sheet
   b. Verify recipient fax number
   c. Call to confirm fax receipt
   d. Disclose minimum amount of information needed for the request
   e. All of the above

Evaluation -Please circle your response.

1. Did this program provide you with a clear understanding of your role and responsibilities for the protection of PHI?	**Very Much**	**Somewhat**	**Not at all**
2. Did this program adequately inform you of resources available for access, use and disclosure of PHI?	**Very Much**	**Somewhat**	**Not at all**
3. Did this program increase your awareness of where safeguards may be applied in your practices?	**Very Much**	**Somewhat**	**Not at all**

Sharp HealthCare
Compliance Education
For Students/ Registry

Components

1. **Module**
2. **Post test**

Sharp HealthCare
Compliance Education
For Students/ Registry

Components

1. **Module**
2. **Post test**

Sharp HealthCare
Compliance Education
For Students/ Registry

PART 1: Sharp HealthCare's Commitment to Principles
PART 2: Sharp HealthCare's Corporate Integrity Agreement

Objectives

Upon completion of the program, you will be able to:

- Understand the Commitment to Principles
- Recognize your responsibility to report compliance violations
- Understand the existence of and obligations under Sharp HealthCare's Corporate Integrity Agreement (CIA) with the Office of Inspector General (OIG).

PART 1: Sharp HealthCare's Commitment to Principles

The Commitment to Principles is Sharp's Code of Conduct for all Employees, Physicians, Volunteers, Vendors and Business Associates. Each year, Sharp HealthCare reviews the Commitment to Principles, and makes changes to keep current with appropriate business practices. As health care professionals, one of the most significant ways we can demonstrate how much we care about those we serve is to visibly display our personal commitment to operating with extraordinary integrity, ethics and morality each and every day.

The Commitment to Principles reinforces Sharp HealthCare's mission and values, and establishes a framework for compliance with all Federal and California laws and regulations.

Principle 1 – Quality of Care
Principle 2 – Professional Ethics
Principle 3 – Conflicts of Interest
Principle 4 – Corporate Assets
Principle 5 – Regulatory Affairs
Principle 6 – Compliance Reporting

Principle 1 – Quality of Care

We are committed to operating with the highest levels of professional, academic and business practices in order to provide high quality care and services.

- We are committed to delivering quality care and services to our patients in a compassionate, respectful and efficient manner
- We treat everyone with respect and dignity
- We offer quality care and services that set community standards and exceed patient expectations

EMTALA

Sharp HealthCare provides every patient seeking medical care at one of our hospitals with an appropriate medical screening exam to determine whether the patient has an emergency medical condition or is in active labor. If the medical screening exam reveals that an emergency medical condition exists, Sharp will provide the patient with the treatment necessary to stabilize the condition.

Principle 2 – Professional Ethics

Day-to-day decisions and actions shall reflect our Mission, our Commitment and our Values. We will conduct business with honesty, fairness and integrity.

Medically Necessary Services

Clear and complete medical documentation and the assignment of appropriate codes are required to ensure that payment is made only for those items or services that are reasonable and necessary.

Principle 3 – Conflicts of Interests

Employees should refrain from activities that create actual or potential conflicts of interests. A conflict of interest is anything that divides an individual's loyalty between the best interests of Sharp HealthCare and those of a patient, supplier, friend, relative, visitor, or competitor.

Examples of conflicts of interests:

- Hiring or contracting with a family member or friend to provide goods or services to Sharp HealthCare.
- Offering or accepting gifts from those doing business or seeking to do business with Sharp HealthCare (except as directed by Sharp HealthCare's compliance policies).

Gifts present certain conflict of interest issues to consider. Sharp defines a **"Gift"** as anything that has any basic economic value, any payment, or any item or service that has a value. Examples include: any favor, tips, gratuities, cash, gift certificates, favorable loans, kickbacks, entertainment, rebate, bribe, tickets to sporting or social events, meals, transportation, education, lodging, or any other consideration of value of any kind provided or received in connection with your position at Sharp HealthCare.

What Is The PhRMA Code?

The PhRMA (Pharmaceutical Research and Manufacturers of America) Code is a guide for relationships between research-based pharmaceutical and biotechnology companies and with healthcare professionals. The Code is recognized by the OIG as a standard in the industry and can be found on the Sharp Intranet Compliance web site.

The PhRMA Code states that items may be offered to healthcare professionals if they are for a nominal value ($100 or less) and for the benefit of patients. For example, an anatomical model for use in an examination room would be considered a benefit to the patient, whereas a VCR, DVD or CD player does not. Items should only be offered on an occasional basis, even if each individual item is appropriate.

- Items of minimal value may be offered if they are primarily associated with a healthcare professional's practice (such as pens, notepads, and similar "reminder" items with company or product logos).
- Items intended for the personal benefit of healthcare professionals (such as floral arrangements, artwork, music CDs or tickets to a sporting event) should not be offered and should not be accepted.
- Payments in cash or cash equivalents (such as gift certificates) should not be directly or indirectly offered to or accepted by healthcare professionals, except as compensation for bona fide services. Cash or equivalent payments of any kind create a potential appearance of impropriety or conflict of interest.

What's Wrong With a Gift?

Nothing. Except if an item of value is being offered or accepted in return for or to induce the referral of a patient for any service that may be paid by federal or state funded health care programs.

- OFFERED OR ACCEPTED: It does not matter what side you are on.
- ITEMS OF VALUE: The amount of value is irrelevant.
- INTENT: There must *not* be an intent to induce a referral or compensate for a referral.

Problematic Gifts

- Cash gifts to gain favor
- Bribes or kickbacks
- Compensation tied to the number of referrals
- Gifts intended to induce the referral of patients
- Gift certificates for weekend get-aways

Acceptable Gifts

- Holiday food baskets (if shared with others)
- Promotional marketing materials
- Recognized Healthcare Professional's Weeks
- Gifts that do not induce the referral of patients
- Sharp sponsored events or community fundraisers

What To Do If You Are Unsure?

Call the Compliance Connection "Hotline" 1-800-350-5022 to report inappropriate offerings or acceptance of gifts.

Principle 4 – Corporate Assets

We commit to excellence within our workplace by respecting the dignity of those we serve, protecting the property of the Sharp HealthCare system, and promoting creativity, innovation, and accountability.

- Financial documents must be prepared accurately, honestly and in accordance with established financial and accounting principles and procedures.
- Private use of Sharp HealthCare's assets and resources for personal use or gain is unacceptable.
- Responsibilities include protecting system passwords from use by any other person.

Principle 5 – Regulatory Affairs

In all our business transactions, we will ensure compliance with all statutes, regulations, and guidelines applicable to Federal and California health care programs, and with Sharp HealthCare's own policies and procedures.

Sharp HealthCare fully cooperates with requests for information from government auditors, investigators or other regulatory agency officials. Likewise, Sharp HealthCare is committed to appropriately disclosing violations of law, regulations or requirements under all government or business contracts to applicable governing entities.

Government Business

- Special care must be exercised when dealing with government officials and agencies.
- Sharp employees who work with government business departments are responsible for knowing and complying with applicable laws and regulations.

Laws & Regulations

Submitting false information or false claims to the government may violate laws, such as:

- *Mail and Wire Fraud Statute* – the use of company mail or wire services, such as fax machines, e-mail or telephone systems to transmit false or misleading information constitutes mail or wire fraud.
- *False Claims Act* – a false claim is any attempt to obtain money from the government by knowingly presenting false or misleading information relating to payment from the government. Examples include knowingly recording or processing any information inaccurately, e.g., changing a beneficiary name, or changing dollar amounts on claims.
- *False Statements Statute* – prohibits a person from making a false or misleading statement or withholding material information in connection with the delivery of services to or payment from the government.
- *Federal Anti-Kickback Statute* – federal Anti-Kickback Statutes impose criminal, civil and monetary penalties not only on individuals who offer a kickback, but also on an organization and its staff who solicit/accept such items. A "kickback" is any money, fee, commission, credit, gift, gratuity, thing of value or compensation of any kind, which is provided, directly or indirectly, to any contractor or subcontractor to improperly obtain or reward favorable treatment in connection with a contract.

Points to remember if contacted by an investigator:

ASK

- If in person – Ask for identification and business card and make copies of both.

- If by telephone – Ask for and write down his/her name, office address, telephone number and identification number.

CALL the appropriate individuals ASAP:

- Your Manager, Administration and the Compliance Department immediately.
- Compliance Department: (858) 499-3138
- Legal Affairs Department: (858) 499-4021

TAKE clear notes and write a list of any documentation presented to the investigator.

TELL

- Tell the representative the truth.
- If you don't know, say you don't know. Don't guess.
- Tell the representative about the location of documents only.
- Tell the representative you would like to have a Sharp representative with you while answering any questions. If appropriate, Sharp can arrange to have a designated individual accompany you.

Principle 6 – Compliance Reporting

Each of us contribute to Sharp HealthCare's continued success of preventing, detecting, and correcting reported violations of the Commitment to Principles, Sharp HealthCare policies, or applicable Federal and California laws. Each Sharp HealthCare employee is responsible for reporting any known or suspected violations of the Sharp HealthCare Commitment to Principles, Sharp HealthCare policies, or applicable Federal and California laws. Our success depends on each of us!

How Can You Make a Difference?

- Go the extra mile! It's more than conducting yourself professionally and ethically.
- Be responsible for those around you! Remind others of the Commitment to Principles.
- We are all dedicated to doing the right thing, but it may not occur to us at times to think about our actions in relation to our Commitment to Principles.
- If an issue does not resolve itself, report it!

Who Do You Report It To?

Several resources have been established to help you report compliance concerns.

- Your supervisor, manager or director
- Your entity's Senior Management, Administration or Compliance Liaison
- Corporate Human Resources (858-499-5228)
- The Compliance Officer (858-499-4015) or Privacy Officer (858-499-3027)
- The Legal Affairs Department (858-499-4021)
- Corporate Information Systems Security Administrator (858-627-5256)
- *Compliance Connection Hotline – if you are unhappy with the results of any of the above, or you prefer to report anonymously, call the Compliance Connection Hotline* (800-350-5022)

How Does the Hotline Work?

- Toll free call
- Option to remain anonymous
- Live operators independent of Sharp HealthCare available 24 hours a day, 7 days a week
- Receive a Call Report Number and call back date to track the status of your call

Your Report

- After your call, the operator will prepare a detailed written report.
- Your report is then sent to Sharp HealthCare's Compliance Officer for timely follow up and investigation.

Compliance Resolution

The Compliance Officer, or a member of the Compliance department will follow up on the details of the call. The status, or resolution is reported back to the Hotline vendor, to relay to the caller on the call back date. All details of a call, the report, and any follow up or investigation shall be confidential, except where disclosure is permitted or required by law.

Strict Non-Retaliation Policy

It is the policy of Sharp HealthCare, and Federal and California law that anyone who, in good faith, discloses information by utilizing the compliance reporting process will not be subject to retaliation by anyone at Sharp HealthCare.

Discipline

Disciplinary action may be taken for any of the following situations:

- Participating in actions that violate the Commitment to Principles or Sharp policies
- Failing to report a possible violation of the Commitment to Principles
- Refusing to cooperate in the investigation of a potential violation
- Retaliating against an individual for reporting a potential violation

The Compliance Connection "Hotline"- 1-800-350-5022

Sharp's success is dependent upon your commitment and integrity

Your Role

- Dedicate yourself to Sharp HealthCare's Commitment to Principles
- Sharp HealthCare's continued success depends upon your commitment and integrity

Resource Guide

Designed to assist you in guidance for reporting and resolving potential violations:

- Your Manager
- Corporate Compliance
- Internal Audit Services
- Senior Leadership
- Legal Affairs
- Compliance Connection Hotline

PART 2: Sharp HealthCare's Corporate Integrity Agreement (CIA)

San Diego Hospital Association (SDHA), Sharp Memorial Hospital, and Sharp Grossmont Hospital have entered into a CIA with the Office of Inspector General (OIG) of the United States Department of Health and Human Services (DHHS) to promote compliance with the Medicare and Medi-Cal health care programs.

Prior to the implementation of this CIA with the OIG, Sharp HealthCare established a corporate compliance program that applied to all Sharp entities and facilities. The CIA accommodates and recognizes many of the elements of Sharp's pre-existing voluntary Compliance Program.

Sharp agrees that during the term of the CIA, it will continue to operate its Compliance Program in a manner that meets the requirements of the CIA. A CIA **mandates** promotion of compliance by Sharp's officers, directors, employees, and contractors with the statutes, regulations, and written directives of Medicare, Medi-Cal, and all other Federal and State health care programs.

The period of the compliance obligations assumed by Sharp HealthCare under the CIA is five years, beginning February 21, 2003.

Sharp shall maintain a Compliance Program that includes the following elements:

I. Compliance Officer
II. Compliance Committee
III. Code of Conduct
IV. Policies and Procedures
V. Education
VI. Compliance Hotline
VII. Ineligible Persons
VIII. OIG Inspection, Audit, and Review Rights

I. Compliance Officer

The Compliance Officer, Paul Belton, shall be responsible for developing and implementing policies, procedures, and practices designed to ensure compliance with the CIA requirements and other Medicare and Medi-Cal health care program requirements.

II. Compliance Committee

The Compliance Committee shall:

- Support the Compliance Officer in fulfilling his responsibilities.
- Assist in the analysis of Sharp HealthCare's risk areas.
- Oversee monitoring of internal and external audits and investigations.

III. Code of Conduct

Sharp shall make the promotion of, and adherence to, the Code of Conduct an element in evaluation the performance of employees. Each year, every employee is required to certify that he or she has read, understood, and shall abide by Sharp's Code of Conduct...our *Commitment to Principles.*

IV. Policies and Procedures

Sharp shall implement written policies and procedures regarding the operation of Sharp's Compliance Program and compliance with Medicare and Medi-Cal health care program requirements.

V. Education

Sharp shall provide at least one hour of general training for all employees annually. This training, at a minimum, shall explain Sharp HealthCare's:

- Existence of a Corporate Integrity Agreement (CIA) and Sharp's obligations there under, and

- Sharp HealthCare's Compliance Program (including our *Commitment to Principles* and Policies and Procedures).
- Cost Report Education – Specific employees involved in cost reporting activities shall receive at least 4 hours of specific training in addition to the general compliance training.
- Coding and Billing Education – Specific employees involved in coding and billing activities shall receive at least 4 hours of specific training in addition to the general compliance training.

VI. Compliance Hotline

Sharp must maintain a compliance hotline to enable employees to disclose to the Compliance Officer, Paul Belton, any identified or potential issues or questions associated with Sharp's policies, practices, or procedures with respect to the Medicare or Medi-Cal programs.

The disclosure program shall emphasize a non-retribution, non-retaliation policy, and shall include a reporting mechanism for anonymous communications for which appropriate confidentiality shall be maintained.

VII. Ineligible Persons

An ineligible person is an individual or entity who is currently excluded, debarred, suspended, or otherwise ineligible to participate in the Medicare or Medi-Cal programs.

Sharp must ensure that all officers, directors, employees, contractors, and agents of Sharp are NOT ineligible persons. Sharp must screen such Persons prior to engaging their services. If Sharp has actual notice that such person has become an Ineligible Person, Sharp shall remove such person from responsibility for, or involvement with, Sharp's business operations related to the Medicare and Medi-Cal programs. If you or anyone you know are an eligible person, you are obligated to report it to your supervisor, manager, human resources representative, and compliance department immediately.

VIII. OIG Inspection, Audit, and Review Rights

The OIG may examine or request copies of documents and/or conduct on-site reviews of any Sharp locations to verify and evaluate:

- Sharp's compliance with the terms of the CIA.
- Compliance with the requirements of the Federal and state health care programs.
- The OIG or its authorized representatives may interview any of Sharp's employees, contractor's and/or agents who consent to be interviewed.
- Employees may elect to be interviewed with or without a Sharp representative present.

EXAM QUESTIONS
COMPLIANCE EDUCATION
FOR STUDENTS/ REGISTRY

Name: _____ **Date:** _____

1. If you are contacted by a regulatory agent by telephone, mail, or in person, you should take which of the following steps:

   A. Bring the matter to the immediate attention of your manager, entity Compliance Liaison, and the Corporate Compliance Department.
   B. Identify the official by asking for an identification badge and/or business card.
   C. If you are unsure of how to answer a question, say so.
   D. All of the above.

2. You are a nurse, and are charting a particular patient's visit based on the physician's diagnosis and treatment plan. The patient, who knows this diagnosis is not covered by her insurance plan, asks you to provide a different (but related) diagnostic code, so that the cost of the treatment will be reimbursed. The physician, in an effort to help the patient maximize her insurance benefits, is going along with the plan. What should you do?

   A. Ask the physician if the diagnosis accurately reflects the proper treatment.
   B. Remind the patient of the importance of accurate medical records.
   C. Report the situation to the Compliance Officer or the Compliance Connection Hotline.
   D. All the above.

3. True or False. The Compliance Connection Hotline is available to all employees to report compliance issues, and reports can be made anonymously if the caller desires.

4. Which of the following is an example of an appropriate gift:

   A. Cash gifts to gain favor
   B. Bribes or kickbacks
   C. Compensation tied to the number of referrals
   D. Promotional marketing materials
   E. Gifts intended to induce the referral of patients

5. The Corporate Integrity Agreement imposed on Sharp HealthCare by the Office of Inspector General of the Department of Health and Human Services obligates mandatory compliance and is for a term of:

   A. One Year
   B. Two Years
   C. Five Years
   D. Ten Years

6. True or False. As an employee of Sharp HealthCare, I understand that I am required to obtain at least 2 hours of general compliance training on an annual basis.

7. To report any actual or perceived violation of the Sharp HealthCare Commitment to Principles, which of the following options would be appropriate?

   A. Contact the President of the American Hospital Association (AHA)
   B. Contact your manager, Entity Compliance Liaison, Senior Management, Legal Affairs or the Compliance Department
   C. Call the Compliance Connection Hotline at 1-800-350-5022
   D. B or C

8. True or False. The Compliance Connection Hotline is available to make a confidential report of identified or potential issues or questions associated with Sharp's policies, practices, or procedures with respect to the Medicare or Medi-Cal programs.

9. True or False. Paul Belton is the Compliance Officer for Sharp HealthCare.

10. As defined by the Office of Inspector General of the Department of Health and Human Services, an Ineligible Person is:

    A. A person who doesn't qualify for Medicare benefits
    B. A person who is barred from participation with insurance plans
    C. A person or entity who is excluded or debarred from participation in the Medicare or Medi-Cal Programs
    D. None of the above
    E. A, B, and D

Information Security Basics

Components

1. **Reading material**
2. **Post test**

Sharp HealthCare

Information Security Basics

Information about Sharp patients, staff, business practices and strategies, are valuable company assets. They need to be carefully managed and protected.

On our computerized systems Sharp has installed:

- Firewalls
- Anti-virus protections
- Personal user accounts
- Workstation security
- Biometric finger scan readers
- Web filters, hacker alerts and other security safeguards; however;

All the technical security that money can buy will not succeed until all network users know, understand and consistently follow basic information security practices.

HIPAA requires security awareness training for all Sharp employees who have been granted accounts and access to the Sharp network and other electronic types of protected health information.

Sharp's program includes:

- Secure Password Management
- Procedures for prevention, detection and reporting malicious software (viruses)
- Procedures for monitoring and reporting evidence of unauthorized account or workstation use
- Security reminders and periodic security updates

HIPAA security regulations apply to Protected Health Information (PHI), which is managed electronically such as clinical data on:

- Computers and laptops
- Web sites and servers
- Portable devises (palm pilots)
- Computerized faxes
- Wireless devices
- Biomedical devices
- Any and all electronic devices which can view/store/process PHI

Information is considered PHI if it contains any one or more of the following data elements:

1. Names	10. Account Numbers
2. All geographic designations smaller than a state, including street addresses, city, county, zip code	11. Certificate and license numbers
3. All elements of dates (except year), including birth date, admission date, discharge date, date of death, and additional rules for ages over 89.	12. Vehicle Identifiers and serial numbers (including license plate numbers)
4. Telephone numbers	13. Devise Identifies and serial numbers.
5. Fax numbers	14. Web Universal Resource Locator (URL)
6. Electronic mail addresses	15. Internet Protocol (IP) address
7. Social Security numbers	16. Biometric identifiers (including fingerprint or voice print)
8. Medical record numbers	17. Full face photographic images and any comparable images.
9. Health plan beneficiary numbers	18. Any other unique identifying number, characteristic or code

Secure Password Management

You are the only one who knows your password.

- Your password will need to be reset if you forget it.
- Help Desk staff cannot view passwords that you have set for yourself.

To guarantee that you are the only one who knows your password:

- The system will prompt you to change your password every 90 days.
- You are encouraged to change your password more often, especially when you have used your password from a public computer external to Sharp.

Examples of secure passwords include an acronym made from a phrase or song:

YWHNB2day = Yes We Have No Bananas 2day

Or

Run short words together and add a number:

(june2thelake – or – Vegaisin05 – or – notime4weeds)

Easy to remember, hard to guess!!

Secure Workstation Management

Never leave a computer workstation unattended unless you have:

- Logged off
- Activated a privacy screen or
- Locked the computer

The automatic time-out function on your workstation is intended to be a back up measure when circumstances prevent an end-user from manually securing the workstation.

Three levels of risk have been assigned to computer workstations:

High Risk Workstations: Workstations open to or accessible by the public that are not under constant supervision, particularly workstations in secluded areas that are not easily or often monitored or workstations located in areas where the presence of non-Sharp personnel is expected, e.g. exam rooms, emergency departments, and workstations on portable cares.

Moderate Risk Workstations: Workstations in non-public areas that are difficult for the general public to access and that are supervised by Sharp staff during all hours of operations, e.g. nursing stations, intensive care units, cubicles, and administrative areas.

Minimum Risk Workstations: Workstations in private offices or lounges that are locked when unattended and are not accessible to the public.

It is risky to use a portable media, e.g. diskettes and CDs on networked workstations, unless they have been pre-scanned for viruses or other malicious code.

Software and hardware should never be installed on any networked devise without knowledge and assistance from the Information Systems Department. Unauthorized installations or configuration changes may cause malfunctions immediately or during future network upgrades and patches.

Contact the Help Desk for assistance with moving devices or equipment on the network.

The World Wide Web should not be used for non-business-related streaming media, such as Internet radio stations, video, TV or interactive games. Technical Web filtering has been activated to prevent access to Web sites:

- That contain inappropriate material
- That permit downloading the background without user permission, e.g. spy ware, remote control, file shares
- That require high bandwidth
- That interfere with clinical systems

If you need access to a blocked site for Sharp **business related** reasons, call the Help Desk to request an exception.

Sharp workstations are currently being upgraded to provide additional security with some new features, including:

- Biometric finger scan devises fro fast authentication
- Automated time-out on workstations when there has been no keyboard or mouse activity for a specified length of time
- Desktop and browser configurations that cannot be changed by end-users.
- New and improved shared clinical workstation to allow users to turn on or reset a workstation between users; your personal user name and password or finger scan must be entered to begin work
- The new CarePoint EMR makes it easier for a clinician to access patient data without having to open and close each application, saving time and increasing accuracy of patient data matches.

Secure Email Management

- Email is one method by which viruses may infect the Sharp network
- Be cautious about opening emailed Web links and attachments from unknown senders—
- If you are not expecting an attachment from a known sender outside of Sharp, verify that it was intentionally sent before attempting to open it.
- Do not send emails to large groups or multiple lists (more than 50 Sharp accounts). These should be submitted to Corporate Communications for review and scheduled distribution.
- When sending email that contains addresses outside of Sharp.com, place the whole distribution list in the 'blind copy' or bcc field. Click on the TO: button to use the BCC: filed. Put your own address in the TO: field.

- Although the Information Systems Department email administrators have implemented measure to reduce spam and unsolicited emails, some still slip through. If you receive one, delete it and forget about it. Do not respond to the email (even to 'unsubscribe'). This tells the sender you open and read unsolicited email…and you'll get more.

Email is not secure!
Do not send PHI through email if it is going outside of Sharp.com unless the file is encrypted or secure.

- It can be altered and/or forwarded
- It can be spoofed or made to look like it came from someone other than the actual sender
- If forwarded or auto forwarded to an email address outside Sharp, (email address that does not end in '@sharp.com') it is transmitted in clear text.
- If available, use more secure means to communicate confidential or sensitive data
- Do not send user names and passwords by email
- Do not send personal demographic data (SSN, employee IDs)
- Keep names and sensitive data out of the subject line
- Delete emails with sensitive data from your email inbox and deleted items box as soon as possible.

Secure Network Management
Manage files by deleting old duplicate or unnecessary files from your PCs F:drive. A full file server is an unavailable file server. If everyone retains only necessary files, server stability will increase. Help Desk analysts can assist you in finding efficient ways to manage your data.

Installing untested an unapproved software on Sharp workstations may interrupt the correct functioning of Sharp business and clinical applications. Certain 'fun' items such as some (not all) wallpaper, cursors, games and music players have hidden functionality which can expose Sharp's confidential files and information or permit unauthorized users to access and view confidential data and files.

Please contact the Help Desk before attempting to install or configure any devise which is used on the Sharp network.

Have you helped a hacker today?
Healthcare workers are in the business of being helpful. The Sharp Experience encourages us to go out of our way to assist people. *"Is there anything else I can do for you? I have the time!"*

Hackers, data thieves and information gatherers know this. A white lab coat and stethoscope or a good story by someone posing as an Information Systems department employee can convince us to provide enough information to cause a security breach.

This method of obtaining access to the network is called '*Social Engineering*'.

Be wise:

- Refer unusual or questionable information requests to your supervisor
- Check for an ID badge if not visible, ask to see it.
- Never disclose your username and password, even to an Information Systems Department worker; if you think someone may know it, reset a new password immediately.

Help Protect Sharp Information
Call the Help Desk if a workstation is behaving strangely or shows signs of unauthorized use.

If you use Remote Access to connect to Sharp's network, you must ensure that your home computer has active and current anti-virus software and that all security patches are applied. Sharp offers home versions of anti-virus and firewall software for all remote access users.

Make sure computer display screens cannot be viewed by patients standing at the desk or sitting in the waiting room.

Notify the Information Systems Department if a computer or laptop is missing; it may be the data on the device, not the device itself, which was the target of the theft.

Refer questions about wireless access and wireless use to the Information Systems Department. Wireless devices should be supervised and protected from unauthorized use.

If someone is asking questions about eh location of the data center or other network equipment, refer the call to the Help Desk.

Facilitate Appropriate Use
If an unknown employee or clinician is demanding to receive clinical data, ask to see their ID badge.

IF a patient or visitor sits down at a Sharp workstation, explain that workstations are not for public use.

Patients are permitted to use their room phone to dial-in to their internet service providers from their own laptops.

Question unknown users at workstations or contact Security at your facility to advise them of the suspicious activity.

Report inappropriate behavior to your supervisor or the Help Desk, e.g., sharing of passwords, allowing unauthorized network use, logging in for someone else.

Report any inappropriate files, pictures or Web sites to the Help Desk, if viewed on a Sharp workstation.

Acceptable Use

Sharp's Acceptable Use of Information & Computing Resources (Policy #13521) contains important information about appropriate behavior required from everyone who is granted accounts for use on the network.

Anyone who is authorized to have a computer account will be required to read and sign an agreement to follow this policy.

The behavior of every network user contributes to the overall confidentiality, data integrity and system availability of Sharp's information assets. Demonstrate your 'network citizenship' by remembering to:

- Log out of your workstation when finished
- Leave workstations secure and ready for the next user
- If you see an unattended workstation in an unsecured state, start up the privacy screen or lock the computer
- If you find **ePHI** printouts lying around, move them to a department designated inbox or escort them to the shred bin.

- If you think someone has tampered with a workstation or if you believe if may have a virus, contact the Help Desk at 858-627-5000
- If someone asks you for you password, give them the Help Desk telephone number instead
- If someone tells you their password, ask them to reset it

Computer Skills
All staff is encouraged to learn and use basic computer skills. You should know how to:

- Reset your password
- Save, find, and open files
- Use email, a web browser, and the applications required for your job
- Manage your desktop when multiple windows have been opened
- Close applications, lock the computer and/or log off
- Communicate a workstation ID and the exact text of an error message when reporting a problem to the Help Desk.

21st Century Medical Records
From one paper chart available in one place at one time to a computer file available at 9,000 workstations at the same time.

Pros

- Record available wherever patient arrives for care
- Record updates are immediately available
- Improved legibility
- Edits and audits improve patient safety

Cons

- Clinicians must acquire/use basic computing skills
- Record availability depends on system stability and 'uptime'
- Technology evolves rapidly, more changes
- New security rules

How do the HIPAA security regs differ from the privacy regs?
HIPAA Security requirements state that Sharp and its workforce must *ensure the confidentiality, integrity, and availability of all ePHI that we:*

- Create
- Receive
- Maintain
- Transmit

Privacy is a right
Confidentiality is a condition
Security is a safeguard

Confidentiality means data or information is not made available or disclosed to unauthorized persons or processes.
Integrity means data or information has not been altered or destroyed in an unauthorized manner.
Availability means data or information is accessible and useable upon demand by an authorized person.

Sharp HealthCare
Information Security Basics
EXAM QUESTIONS

Name: _____ **Date:** _____

1. Who is responsible for information protection and data security?
   A. The Information Systems department
   B. The Sharp Privacy Officer and Information Security Officer
   C. Everyone who has an account on the Sharp network
   D. Sharp's Legal Services department

2. What is ePHI?
   A. Everyone's Personal Health Information
   B. Protected Health Information which is managed electronically
   C. The same thing we learned about in the Privacy training
   D. A and C

3. Passwords must be secure
   A. To protect Sharp information on the network
   B. To protect my personal files and information
   C. To prevent others from using my account
   D. All of the above

4. Sharp has upgraded workstations security with these new features:
   A. Biometric finger scan devices
   B. Automatic time-out functions
   C. A, B and D
   D. Re-designed shared clinical workstations

5. E-mail users need to understand
   A. Appropriate use of e-mail in the workplace
   B. Proper management of attachments and Web links from unknown senders
   C. Policy and restrictions on use of e-mail to send ePHI to addresses outside of @sharp.com
   D. All of the above

6. The secure management of e-mail
   A. Is part technical and part end-user behavior
   B. Can be completely managed by technical measures
   C. Is dependent on whether or not e-mail addresses are exposed on the Internet
   D. Makes it private and protected

7. Installing unapproved software or devices can result in:
   A. Introduction of malicious code onto the Sharp network
   B. Incompatibilities which disrupt proper function of workstation, application or network
   C. Exposure of Sharp's confidential files and information to unauthorized users.
   D. All of the above

8. Who is permitted to use Sharp workstations and computer devices?
   A. Sharp workforce members who are eligible and authorized to have accounts
   B. Visitors, patients, family members and guests who ask permission
   C. Anyone, as long as they use SharpPC
   D. A and B

9. Warning signs of social engineering may include:
   A. Urgent-sounding requests to use your login or to print out ePHI information
   B. Demands to disclose your username and password
   C. Conversations requesting information about how the network works and where the data center is located
   D. All of the above

10. HIPAA Privacy regulations address confidentiality of all PHI while HIPAA Security regulations address
   A. Confidentiality of electronic PHI only
   B. The right to maintain privacy of patient information
   C. Safeguarding confidentiality, Integrity and Availability of ePHI created, received, maintained and transmitted by Sharp
   D. None of the Above