

Intake and Output Help Sheet

1 ounce = 30 cc

16 ounces = 480 cc

Water pitcher or large Styrofoam cup

4 ounces = 120 cc

Juice container

8 ounces = 240 cc

Small coffee cup

Intake and Output Competency

1. Calculate Mrs. Ander's total intake for breakfast if she ate and drank the following:
 - 4 ounce container of orange juice- she drank $\frac{1}{2}$
 - 120 cc of milk
 - 1 egg
 - 2 slices of toast
 - 2 slices of bacon
 - 1 cup of coffee (large Styrofoam cup)

Total intake: _____

2. What is the total output for Mr. Kramer? _____
Voided 400 cc urine; emesis (100cc), urine (250), urine (300)
3. What is the total intake for Ms Friedman? _____
IV 1000cc
IV (250 remaining of 500cc bag)
Breakfast 420 cc
Lunch 300 cc
Dinner 585 cc

Name

Agency

**DEPARTMENT OF NURSING
REGISTRY STAFF ORIENTATION QUIZ**

1. Fill in the blanks CODE Red steps:
R _____
A _____
C _____
E _____
2. To page a "CODE Red," dial _____.
3. The phrase Harbor uses to notify staff that a patient needs resuscitation is _____.
To page the "Alert Team," dial _____.
4. T or F A patient's emotional state or cultural background will affect how you communicate with him or her.
5. The most important element of infection control is good _____ after each patient procedure.
6. List 2 ways to protect yourself from being exposure to infected body fluids.
a. _____
b. _____
7. Paging the Nursing supervisor is done by dialing _____.
8. T or F If a piece of equipment is not functioning, you should label it and immediately remove it from service.
9. MSDS sheet is found in (circle correct answer)
a) red notebook b) blue notebook c) yellow notebook d) green notebook
10. Harbor will not permit patients to be subjected to abuse by anyone. Types of Abuse includes:
1. _____
2. _____
3. _____
11. T or F Maryland law provides that anyone who physically abuses a vulnerable adult may be imprisoned for 5 years.
12. Failure to report abuse may result in a _____ fine and will be _____ from Harbor.
13. T or F Restraining a patient may be done with a sheet or gauze
14. T or F All alternatives to restraint use must be documented first
15. T or F Patients in 4 point restraints must have a sitter
16. T or F Chest/Vest restraints are encouraged
17. T or F You must complete this quiz and return it to the person who will sign your time slip before your time slip may be submitted.

Name
Signature needed on page 18, 19, 20, 21 and 26

Agency
5/1/2006 19

Harbor Hospital

The information you received upon coming to Harbor has been compiled to make your experience here rewarding for you and for us. To comply with regulatory standards, we ask that you sign this form indicating that you have read and understand the material presented (Fire, Infection Control, Mission, Vision, Values, Alert Team, Emergency Preparedness, Security, Incident Reporting, Patient Rights, Hazmat). You also affirm that your CPR (if applicable), and PPD (no infectious S and S) are current.

Thank you,

The Nursing Department of Harbor

Print Name: _____

CPR Expiration Date: _____

Drivers License #: _____ State of Issue: _____

Signature: _____

Date: _____

Registry / Agency: _____

Please return signed form to Nursing Supervisor.

HARBOR HOSPITAL
AGENCY/CONTRACT Sitter/CNA PERFORMANCE EVALUATION

Name: _____ Date: _____

Agency: _____

The nursing supervisor or designee will complete the following evaluation for each agency nurse:

Rating Scale: S = Satisfactory

U = Unsatisfactory

*A rating of U must be followed by a comment and reported to Nursing Supervisor

Topic	Rating	Comments
1. Adheres to policies and procedures specific to Harbor Hospital (HH).		
2. Is tactful and effective in communicating with staff, patients, and families.		
3. Aware of own abilities and limitations: asks questions.		
4. Responds appropriately to emergency situations.		
5. Refers problems appropriately.		
6. Demonstrates professional demeanor and attire.		
To be completed by Nursing Supervisor/PCM: Overall Performance _____ Satisfactory _____ Unsatisfactory	_____	
Recommended for Continued Assignment _____ Yes _____ No	_____	
	Sign. of Nsg. Supv./PCM	Date
Comments required for overall unsatisfactory performance:		

HARBOR HOSPITAL
CONFIDENTIALITY & SECURITY POLICY

Policy

All patient and organizational proprietary business information including, but not limited to medical records shall be confidential, current, accurate and made available only to authorized users. The confidentiality, security and integrity of data and information are maintained. The patient health record is the property of the Medstar site and shall be maintained to serve the patient and health care providers in accordance with legal, accrediting and regulatory agency requirements. The patient/enrollee has an interest in the information and is entitled to the protection of that information. All information residing on computer systems of Medstar Health management will determine appropriate level of security and confidentiality for data and information. Collection, storage, and retrieval systems are designed to allow timely and easy use of data and information. Collection, storage, and retrieval systems are designed to allow timely and easy use of data and information without compromising its security and confidentiality. Records and information are protected against loss, destruction, tampering, and unauthorized access or use.

VIOLATION OF THIS POLICY AND THE PROCEDURES DESCRIBED HEREIN WILL: RESULT IN DISCIPLINARY ACTION AND/OR POSSIBLE TERMINATION AND/OR LEGAL ACTION BY MEDSTAR HEALTH. PENALTIES UNDER MARYLAND LAW FOR UNAUTHORIZED OR INAPPROPRIATE DISCLOSURE OF PATIENT INFORMATION INCLUDE FINES UP TO \$250,000 AND/OR IMPRISONMENT FOR UP TO TEN YEARS.

A confidentiality Statement will be signed by all persons employed by Medstar Health and other approved users (see "Definitions" pg. 5). The agreement states that the employees or persons accessing Medstar Health information will not release or utilize any confidential or proprietary information gained during their entire period of employment or affiliation to anyone nor access information not appropriate for their position. This agreement will survive termination of employment or affiliation regardless of the reason for separation.

1.0 Procedures

1.1 All patient information shall be stored in a physically secure media under the immediate control of the Health Information Management Department of the Director of Information Services as the case may be.

1.1.1 Patient records shall be retained according to applicable legal, accrediting and regulatory agency requirements and for the length of time required or otherwise defined by Medstar Health policies.

1.1.2 Whenever medically feasible, written consent will be obtained from the patient or appropriate representative prior to release of information.

1.1.3 E-mail and the Internet are not permitted for purposes of transmitting Medstar patient information (see also Medstar Health Information Systems policies on Internet Use and Electronic Messaging Systems).

1.1.4 Original medical records may not be removed from the premises except upon order of a subpoena or court order.

1.1.5 Except for routine patient transfer arrangements and bona fide medical emergencies, all requests for patient information should be referred to the Health Information Management Departments to assure adherence to proper procedures.

1.1.6 When photocopies or faxes of patient information are provided to authorized external users for immediate patient transfer or emergency treatment elsewhere they will be accompanied by a cover sheet or statement:

- 1.1.6.1 Prohibiting use of the information for other than the stated purposes
- 1.1.6.2 Prohibiting disclosure by recipient to any other party

(Authorized FAX cover sheet forms can be obtained from the Health Information Management Department at each Medstar site)

1.1.7 All efforts will be taken to protect medical information from access in patient care settings or public areas by keeping information from records, computer screens and conversations about patients confidential.

1.1.8 General and public access to the main areas storing or archiving patient records or information shall be limited to authorized Health Information Management or Information Systems personnel.

1.1.9 Only those health care personnel directly involved in providing patient care or other individuals authorized by administration in the performance of their duties shall have ready and accessible access to medical records and patient information.

1.1.10 Disposal of secondary source data, electronic or physical copies of records, patient work lists, census data, payroll and proprietary information should be by shredding. Medstar approved recycling program or other secure and approved method.

2.0 Data Integrity and Security Breaches

2.1 Any real, potential or suspected breach of patient confidentiality is considered an emergency situation and must be reported to the area manager first, then to the Information Services Help Desk if a system breach has also occurred. Immediate arrangements will be made to remove access by the violator. Follow-up investigations will be conducted by the department manager, Human Resources, the local system administrator and the Medstar Information Systems Security Administrator, appropriate recommendations and actions will follow. Risk Management will be notified as appropriate.

2.2 Students or volunteers violating this policy will be dismissed from all Medstar programs.

In addition, breaches in the security of proprietary Medstar business, payroll or credit history data will also be reported to the manager of the business unit and to the Medstar Legal Department.

3.0 Assigning ID's and Passwords

3.1 In addition to the Statement of Confidentiality, those with access to computer information will sign an additional password authorization agreement. Departments responsible for each application will determine the levels of access, who can change data for each data element and if access to data should be limited or restricted in any way.

3.2 Requests for ID's and passwords for new users are submitted by the manager or training specialist on the appropriate forms. Passwords coded for access to systems containing patient information will be put into the applicable system security user table and communicated back to the employee in a sealed confidential envelope. Passwords for access to patient information screens will not display on the screen at time of sign-up. The area managers will receive notification once codes have been assigned.

- 3.3 Should an employee suspect that his/his password has become known by another individual it is that employees' responsibility to report this information to both the Information Systems Help Desk and the area manager as soon as possible. The ID and password in question will be deactivated and a new one will be generated.
- 3.4 It is the responsibility of area managers to immediately report any changes in user status to the Information Systems Help Desk and/or the appropriate system administrators. When employees are terminated, it is imperative that passwords be removed from circulation as soon as possible. The System Security Administrator will conduct routine audits of terminated employees to assure deactivation of ID's and passwords.
- 3.5 Inappropriate use of ID's, passwords or assigned security levels for the purpose of accessing information other than that specifically needed to perform the approved business function is a violation of this policy. Likewise, using another's ID or password or loaning one's own ID or password to another individual is forbidden.

4.0 Education/Orientation of Users

- 4.1 All system users are to receive education and training regarding aspects of security and confidentiality, which is specific to the applications and technology they are authorized to use. Information will be provided concerning security issues related to technology such as networks, modems, remote access and back-up routine. Content will include but not be limited to:
 - 4.1.1 Identification of information that must be secured and a review of the methods available
 - 4.1.2 How to identify potential security breeches and methods to prevent breeches
 - 4.1.3 Methods to dispose of system output, e.g. reports, disks, etc.
 - 4.1.4 What to do if breech is suspected
 - 4.1.5 Use of ID and password
 - 4.1.6 Time frame and schedule of automatic password changes
 - 4.1.7 Review of personal access pathways and process to follow if modification is necessary.
- 4.2 Validation of initial system competencies for patient information systems will be by direct observation, paper and pencil, quizzes and/or other means to be determined by the system administrator for the relevant application.
- 4.3 Maintenance of continuing competence, including confidentiality/security policy review will be pan of the annual employee performance review.

5.0 Electronic Signature

- 5.1 Electronic signature may be used to authenticate computer-based patient records in accordance with applicable law and accreditation guidelines. System administrators will submit procedures for use of electronic signature for approval by the Medstar Information Systems Security Administrator.
- 5.2 Use of electronic signature is noted on the patient medical records and permanently stored electronically within the system. Individual use of electronic signature will be denied unless written agreement is obtained that no other individual has access to or will use the computer key. Privilege to use electronic signature will be removed is abuse is suspected.

6.0 System Back-up and Recovery

- 6.1 All Medstar Information Systems applications are backed up routinely standard industry methods. All users of computers including PC's are responsible for backing-up files for their individual systems on a regular basis.
- 6.2 Back-up media must be stored in a safe place remote from the server. Local system administrators must conduct back-ups and storage for system not managed by the Medstar Information Systems Department. All equipment used to access Medstar Health systems regardless of ownership, must be kept in an environment that meets the vendor guidelines for smooth and efficient system performance.
- 6.3 System managers must develop a plan to provide access to current information in the event system data is temporarily unavailable.
- 6.4 Safe storage of data (paper, tape, optical disk, etc.) is the responsibility of the manager of the system. Back-up storage of current and archival data should be kept remote from the machine in the event of a physical disaster or power failure.
- 6.5 Should a disaster occur resulting in the loss of patient or critical business information, the most advanced technology available will be used to recover the data.
- 6.6 Utilizing back-up and data recovery routines for lost transactions is the ongoing responsibility of the system manager.
- 6.7 Information systems containing patient treatment data should be backed-up daily; other systems should be backed-up as determined to be necessary by the business unit.

7.0 Virus Protection

- 7.1 It is prohibited for employees and other users to install software onto Medstar Health System computers unless prior approved by the Information Systems Department; after approval installation of software must be done by the Information Systems Department.

Violation of this procedure may result in disciplinary action should corruption of files result from installation of unauthorized software.

- 7.2 Medstar provides anti-virus software which must be kept running at all times. Viruses unknowingly transmitted through the Internet, electronic messaging and by importing software or programs in Medstar Health computers from outside sources must be eliminated immediately. The Medstar Information System Help Desk will notify users of how to detect viruses as they are suspected to have entered the system. Symptoms suspicious of virus contamination may include changes in file sizes or content, unexplained appearance of new files, frequent system crashes or incorrectly routed messages and must be immediately reported to the Information Systems Help Desk.

8.0 Definitions

- 8.1 Confidential Information: Specifically includes but is not limited to all patient information, employee information, credit history files, passwords issued, organizational business and proprietary vendor information.
- 8.2 Medstar System: Includes Medstar Health and its affiliated organizations including Medstar Care and the Medstar diversified entities.
- 8.3 Proprietary Information: Includes but is not limited to knowledge of exclusive information utilized for Medstar organizational business or by affiliated Medstar vendors.

- 8.4 Release of Information: Refers to but is not limited to any patient or proprietary business information regardless of the storage media including but not limited to paper records, electronic messaging, verbal or written communications and computer system data and records.
- 8.5 Software: May include but is not limited to proprietary or pirated software, screen savers, scrapers, games, personal software, stand alone software products, demo disks and educational software.
- 8.6 Users: System users may be defined as physicians, GME resident staff, employees of Medstar Health, contractual personnel, temporary personnel, vendors, volunteers and students based in Medstar facilities or others working on behalf of Medstar regardless of location.

Print Name: _____

Signature: _____ Title _____

Date: _____

HARBOR HOSPITAL
Department of Nursing

AGENCY/PATIENT CARE ASSOCIATE
SKILLS CHECKLIST

Name _____

Date _____

The following skills are expectations at Harbor Hospital and must be checked off as competent before working.

Skill/Competency	Signature of Evaluator	Date
<p>1. <u>ASEPTIC TECHNIQUE</u></p> <ul style="list-style-type: none"> A. Properly washes hands before and after patient care. B. Performs sterile gloving without contamination. C. Opens sterile packages and maintains sterility. D. Follows procedure in applying dry sterile dressing 		
<p>2. <u>ELIMINATION</u></p> <ul style="list-style-type: none"> A. Assists patient with bed pan, urinal, & commode while maintaining privacy & safety. B. Provides hygiene for patient with indwelling catheter; proper position to maintain free flow of urine C. Applies & maintains condom catheter & observes & reports skin condition. D. Accurately measure & records urine from indwelling catheter. E. Removes indwelling catheter following correct technique. F. Performs ostomy care using correct equipment & procedure. 		
<p>3. <u>DRAINS/SUCTION</u></p> <ul style="list-style-type: none"> A. Empties & accurately measures drainage from a closed suction device (Gomco/Jp/Hemovac) & re-establishes suction. B. Assists in setting up continuous & intermittent wall suction. 		
<p>4. <u>GLUCOMETER</u></p> <ul style="list-style-type: none"> A. Glucometer following established procedures & records/notifies nurse of the results. 		
<p>5. <u>INTAKE/OUTPUT</u></p> <ul style="list-style-type: none"> A. Records oral intake & urine/drainage output accurately. Adds shift totals correctly. 		
<p>6. <u>ISOLATION</u></p> <ul style="list-style-type: none"> A. Applies & removes isolation attire using correct technique. B. Uses mask, gloves, &/or gown in appropriate situations. 		

<p>7. <u>PROTECTIVE DEVICES & FALLS PREVENTION</u></p> <ul style="list-style-type: none"> A. Applies & removes limb & chest restraints following established procedure. B. Documents patient care on Restraint Flow Sheet. C. Follows procedure for falls prevention and documents interventions appropriately. 		
<p>8. <u>PULMONARY SUPPORT</u></p> <ul style="list-style-type: none"> A. Assists with following as directed by RN & report results/observation: <ul style="list-style-type: none"> ▪ Coughing & deep breathing ▪ Incentive spirometry ▪ Oxygen therapy ▪ Pulse oximetry 		
<p>9. <u>SPECIMENS</u></p> <ul style="list-style-type: none"> A. Collects the following specimens using correct procedure: <ul style="list-style-type: none"> ▪ Sputum ▪ Stool ▪ Urine (24 hour) ▪ Urine (routine) ▪ Urine (mid-stream clean catch) ▪ Urine (from indwelling catheter) ▪ Urine (straining for calcoli) 		
<p>10. <u>VITAL SIGNS</u></p> <ul style="list-style-type: none"> A. Accurately measures & records vital signs (T,P,R,BP) and records pain report. B. Weights patients & records results. 		