NC Department of Health and Human Services Work Area Physical Safeguards Assessment for HIPAA Privacy Compliance

1 PURPOSE

To provide a questionnaire that can be used to assess various work areas for physical safeguards to ensure the privacy of individually identifiable health information (IIHI) that is used or maintained within that area.

2 SCOPE

The focus of the questionnaire provided herein is to identify physical work areas that contain individually identifiable health information and to determine whether such information is adequately protected through physical safeguards. Assessment shall include the physical protection of IIHI kept in hard copy form such as paper, diagnostic images, and archived media such as microfilm, microfiche, compact disc, tape, etc. Confidential information that is accessible through computer monitors and medical equipment must be assessed as well.

3 INSTRUCTIONS

3.1 Step One: Pre-Assessment Tasks

1) Identify all areas where individually identifiable health information is routinely used or stored, including offices, treatment areas, administrative areas, public areas, etc. Results from the Business Information Flow Assessment (BIFA) may be used for this task.

2) **Restricted** or **sensitive** work areas where IIHI is stored, used, and/or disclosed may require physical safeguards that afford a higher level of security and protection. Examples of areas that require special attention include:

   - Medical Record Departments
   - Nursing Stations
   - Therapist/Clinician Offices
   - Patient Accounting Departments
   - Admissions
   - Utilization Review
   - Risk Management
   - Radiology
   - Clinical Laboratory
   - Outpatient Clinics
   - Other areas where health information is routinely stored

3.2 Step Two: Assessment Questionnaire

Complete one *Physical Safeguards Assessment Questionnaire* for each room/area in each building that meets the criteria described above in the *Pre-assessment Tasks* section. Assessment should include a review of the effectiveness of current physical safeguard measures for protecting highly sensitive information. The level of effectiveness will depend on the procedures and practices that are being used. For example:

- Are keys and combinations/codes carefully controlled?
- Are access cards available for more than one person's use?
- Is secretive entry possible (e.g., unattended areas accessible to unauthorized persons)?
- If combination/coded locks are used, can entry be observed by unauthorized individuals?

If resources are limited, use the BIFA results to distinguish high-risk areas and prioritize locations to ensure high-risk areas are assessed first. High-risk areas are those where workgroups use or maintain the following types of information:

- Administrative – incident reports; Cancer Registry
- Financial – claims information
- Employee/Staff Information – employee health records; employee assistance program information
- Utilization Review – FL-2/MR-2 forms; worksheets, reviews, reports
- Clinical Information – complete medical records; assessments/reports; diagnosis/procedure; discharge summary; exams/evaluation/assessments/histories; laboratory data; medication error reports; pathology reports; psychological records and testing reports; psychotherapy notes; radiology reports

The gray block in the 'Response' column on the questionnaire indicates a gap in physical safeguards for protecting the privacy of individually identifiable health information and requires further analysis with possible remediation.

3.3 Step Three: Post Assessment Tasks

Use the 'Remediation Options' column of the *Physical Safeguards Assessment Questionnaire* (see next section) to determine possible solutions for identified problem areas. Your agency may determine that an option other than those listed is appropriate. Record the option determined to be the best solution in 'Remediation Implemented' column. Note that remediation solutions you implement may need to be reinforced by agency policies, procedures, and training.

Physical safeguard deficiencies (e.g., repositioning a desk so that PC screen is not visible to public view/need for locking file cabinet) that cannot be immediately remediated should be reported to your Agency Privacy Official for disposition. Those deficiencies that require capital improvements (i.e., structural changes such as the installation of doors, locks, proximity card systems, walls, etc.) must be processed according to DHHS and State Construction requirements, using the *Proposed Repair and Renovation or Capital Improvement Project (OC-25)*.

Note: Each agency must select the level of safeguards that are appropriate to ensure the privacy and physical safeguarding of IIHI.

4 PHYSICAL SAFEGUARDS ASSESSMENT QUESTIONNAIRE

Click icon below to open Physical Safeguards Assessment Questionnaire

****End of Document****