TITLE: Signature Stamps, Password Sharing, Authentication of Electronic Reports and Scanned Signatures

POLICY/PURPOSE:
To provide guidance to minimize compliance risks associated with: signature stamps, password sharing, electronic authentication of medical records and scanned signatures. This policy is applicable to all locations on campus and all off-site locations where UF faculty, residents, medical students, advanced practice professionals, clinical staff and UF or UFJPI personnel are involved in clinical patient care services, processing claims for reimbursement, or assisting with medical record documentation.

DEFINITIONS:

PROCEDURE:

1. The use of a signature stamp may decrease the amount of time required to sign documents and medical records where there are numerous documents to sign and/or when the documents appear to be "standard" in nature. However, the risks of using signature stamps include the unauthorized use of the stamp by others (e.g., clerical staff and/or other practitioners) on documents that the physician or practitioner has not reviewed for content (e.g., patient and/or billing records) and the possibility of the stamp being stolen. Generally speaking, most insurance carriers do not permit the use of signature stamps or require the signature stamp to be initialed by the provider.

2. Due to variances in insurance carrier guidelines and the potential for misuse, signature stamps are prohibited and must not be used unless permission is granted specifically by the UF or UFJPI Human Resources Department in accordance with the *Americans with Disabilities Act* or the *Rehabilitation Act of 1973* (and various updates to these laws). Compliance must be notified when an accommodation is granted for the use of signature stamps.

3. In this electronic age, other mechanisms similar to signature stamps may be available. Another example of prohibited behavior would be copying a "scanned" provider signature and pasting that image to the signature line of patient and or billing records (*e.g.*, dictated clinic notes).

4. **Passwords for electronic health record systems must not be shared and the responsibility for authenticating reports must not be delegated to anyone.** The provider assigned the password ultimately is responsible for the information contained in the electronically authenticated report.

REFERENCES: CMS. Medicare Program Integrity Manual 100-08. Ch. 3. § 3.3.2.4.

APPROVED BY: Maryann C. Palmeter
Director, Office of Physician Billing Compliance