Policy on Requesting New User Accounts and Access to Clinical Systems

Effective 10/30/2024

Policy Statement

Requests for access to clinical systems are made through the SOD Health Information and Business Systems (HIBS) ticketing system unless otherwise excepted below.

Rationale:

This policy outlines the procedures for creating new accounts and granting access to clinical systems, including SALUD, MiPACS, Dolphin, I-CAT, J Morita, Carestream, Osteoid, 3Shape, and Oryx. It is essential to follow these guidelines to ensure authorized access, compliance with privacy regulations, and proper account management within the School of Dentistry (SOD).

Procedures:

1. **Submitting a Request:**
    - All requests for new accounts or access must be submitted through the HIBS Helpdesk ticketing system at **https://go.uab.edu/hibshelpdesk.**
    - Each request must include:
        - User's full name
        - Role (e.g., student, faculty, or staff)
        - Department or program
        - Clinical system(s) for which access is requested
        - Access level required (for staff roles, specify type and level of access)
        - Expected duration of access, if temporary
    - Approval is required from the Registrar's office for students or from the faculty chair or department head for staff and faculty.
2. **Account Creation and Access Provisioning:**
    - Upon receipt and approval of the request, HIBS will create the necessary accounts and grant access based on the specified role and access level.
    - Access to any clinical system will only be granted after the user has completed the required HIPAA training, as mandated by the SOD.
3. **Notification of Role Changes and Separations:**
    - Departments must notify HIBS of any employee separations or role changes as soon as possible to facilitate timely deactivation or adjustment of access.
    - HIBS will terminate or modify access for individuals who are no longer affiliated with the SOD or have experienced a role change affecting their system access needs.
4. **User Responsibility and Best Practices:**
    - All users are responsible for ensuring the security and confidentiality of the information accessed in these clinical systems.

  - Users should always log out of each clinical system once they have completed their work to prevent unauthorized access to patient information or other sensitive data.
  - Users should guard against unauthorized view of data on monitors that are visible to others.

Compliance:
Non-compliance with this policy, including failure to follow proper access request procedures or mismanagement of system access, may result in disciplinary action, including restricted access to clinical systems.

Implementation:
The Associate Dean for Clinical Affairs and the HIBS Manager are responsible for ensuring the implementation and adherence to this policy.

Effective Date: 10/30/2024