| **Title:** | *Rules of Behavior for UABHS Information Systems* | | |
|---|---|---|---|
| Author: *David Gardner* 12/08/09<br>David Gardner Date | Author:<br>NA Date | Distribution:<br>Health System Wide | |
| Endorsed: *See Interdisciplinary Collaboration* Date | Endorsed:<br>NA Date | Pages 1 of 5<br>Written 12/08/09<br>Reviewed<br>Revised 01/10/11<br>Issued 04/05/10 | |
| Approved: *Will Ferniany* 04/07/10<br>Will Ferniany, PhD Date<br>CEO, UAB Health System | Approved:<br>NA Date | | |
| CAMH Ref#: NA | | Discontinued: | |

**Associated Diagnosis/-Cross-References (CR):**

**Data Security (CR)*
**Password Reset (CR)*
**Confidentiality of Information (CR)*
**Use & Disclosure of Health Information (CR)*
**Use & Disclosure of Health Information for Fundraising (CR)*
**Use & Disclosure of Health Information for Marketing (CR)*
**Information for Research (CR)*
**Information Systems & Network Access (CR)*
**Use of Portable Computing & Storage Devices (CR)*
**Information Security Disciplinary Action (CR)*
**Information Security & Privacy Incidents (CR)*
**Information System Account Management (CR)*
**Consent to Photograph, Video or Audio Record (CR)*
**Security & Privacy Incident Response (CR)*
**Electronic Signatures (CR)*
**Internet & Email Use (CR)*
**Media Reallocation & Disposal (CR)*

1. **PURPOSE:** To effectively communicate information security guidelines to all users of University of Alabama at Birmingham Health System (UABHS) information systems.

2. **PHILOSOPHY:** It is our belief that UABHS employees and contracted personnel must be informed concerning the wide range of information security policy pertaining to them in order to ensure compliance and individual accountability.

3. **ASSOCIATED INFORMATION:**
   - 3.1. **Definitions:**
     - 3.1.1. ***Information System*** - An integrated set of components (i.e. people, hardware, and/or software) for collecting, storing, processing, and/or communicating information for a specific purpose.
     - 3.1.2. ***Electronic Signature*** - The attribute that is affixed to an electronic document to bind it to a particular entity.

4. **STANDARDS:**
   - 4.1. All persons, as a condition of access to UABHS information systems, shall be required to sign (physically or electronically) a Rules of Behavior form. *See **Attachment A** for a copy of this agreement.*
     - 4.1.1. As part of the orientation process, all Health System employees shall be informed on how to complete an electronic acknowledgement or receive a copy of the signed acknowledgement, which shall be placed in the employee's personnel file.
     - 4.1.2. As part of the Health System contract process, a copy of the Rules of Behavior form shall be attached to the applicable contract documentation.
       - 4.1.2.1. Vendor representatives or other external personnel who are not able to complete an electronic acknowledgement, must submit a signed copy of the Rules of Behavior form to the appropriate UABHS departmental manager (where the service is performed) or HSIS project coordinator before access to UABHS information systems is granted.
   - 4.2. All UABHS information system users shall renew their acknowledgement of and their signature on the Rules of Behavior form on an annual basis.
     - 4.2.1. As part of the Health System employee evaluation process, supervisors shall verify that employees under their supervision have renewed their acknowledgement of the Rules of Behavior form.

5. **REFERENCES:** None

6. **SCOPE:** This standard applies to all areas of the Health System.

7. **ATTACHMENTS:**
Attachment A: Rules of Behavior for UABHS Information Systems Form
***NOTE:*** *When using this form, print from the "Form's" section on the SPP/SCR Web, not from this standard.*

## INTERDISCIPLINARY COLLABORATION

| | |
|---|---|
| *HS Corporate Compliance Committee* | *11/12/09* |
| *Information Security Privacy Committee* | *02/11/10* |
| UAB Health System Committees | Date **Reviewed** |
| *None* | |
| Physician / Medical Committees | Date **Reviewed** |
| *None* | |
| Committees / Councils | Endorsement Date |
| *Kathleen Kauffman, Legal Council* | *11/10/09* |
| *Patricia Pritchett, Legal Council* | *10/11/09* |
| *Connie Pruett, Director, UAB Hospital Human Resource Management* | |
| *Marty Box, Director, Health Services Foundation Human Resources* | |
| *Karen Burleson, Director, Callahan Eye Foundation Hospital Human Resources* | *11/10/09* |
| *Cindy Ryland-Holmes, VIVA Health Human Resources* | *11/11/09* |
| *Teresa Evans, Compliance Manager, VIVA Health* | *01/14/10* |
| *Joan Hicks, CIO, UAB* | *10/11/09* |
| *Terrell Herzig, Information Security* | *10/11/09* |
| *Jennifer Cole, HSIS* | *10/11/09* |
| Department(s) | Endorsement Date |

## Approved by:

| | |
|---|---|
| *Michael Waldrum* | *04/02/10* |
| Michael Waldrum, MD, MS, CEO, UAB Hospital | Approval Date |
| *Don Lilly* | 04/07/10 |
| Don Lilly, Interim CEO, Callahan Eye Foundation Hospital | Approval Date |
| *Anthony Patterson* | 04/02/10 |
| Anthony Patterson, COO, UAB Highlands | Approval Date |
| *Cynthia Brumfield* | 04/05/10 |
| Cynthia Brumfield, MD, Chief of Staff, UAB Hospital | Approval Date |

## Tracking Record

| Action | | | | Reasons for Development/Change of Standard | | | | | | | Change in Practice | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Developed | Reformatted | Reviewed | Revised | Required Review | Relevance | Ethics | Legal | New Knowledge | QA/I | Risk | No | Yes | Comment/ Explanation of Impact |
| X | | | | | X | | | X | | X | | X | *Establishes new practice* ***Quality revision to include Wireless Networking*** |
| Supersedes: | None | | | | | | | | | | | | |
| File Name: | Rules of Behavior for UABHS Information Systems I# 1115 | | | | | | | | | | | | |
| REVISIONS: Consistent with Joint Commission Standards, this standard is to be reviewed at least every 3 years and/or as practice changes. | | | | | | | | | | | | | |

Attachment A:

UAB HEALTH SYSTEM

# Rules of Behavior for University of Alabama Birmingham Health System (UABHS) Information Systems

The following Rules of Behavior apply to all users of UABHS information systems regardless of organizational affiliation. These rules are intended to communicate IT-related policy in a concise manner and are consistent with policy detailed in approved UABHS documents. They do not replace or supersede official UABHS standards, policies, and procedures that are made available on the Standards & Clinical Resources (SCR) web site at: https://scr.hs.uab.edu/ and the UAB HIPAA web site at: http://www.hipaa.uab.edu/standards.htm.

**Definitions:**

Information System - An integrated set of components (hardware and/or software) for collecting, storing, processing, and/or communicating information for a specific purpose.

Portable Devices – Equipment capable of processing, storing or transmitting electronic data designed for mobility. Such devices may interact with other networked systems, the internet, desktop personal computers via some form of interconnection and/or synchronization process. They include but are not limited to, personal digital assistants (PDAs), cell phones, text messaging pagers, cameras, and peripherals that employ removable media (e.g., CDs, DVDs, USB flash memory drives, memory cards, external hard drives, and diskettes).

Sensitive Information or data - Any information that may only be accessed by authorized personnel. It includes Protected Health Information, financial information, personnel data, trade secrets and any information that is deemed confidential or that would negatively affect the Health System if inappropriately handled.

Phishing - The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

**System Access & Accountability:**

- I understand that my access to UABHS information systems is contingent upon my acknowledgement of this Rules of Behavior form.
- I understand that my user account is equivalent to my legal signature, and I will be accountable for all work done under this account.
- I understand that I am given access to only those systems for which I require access to perform my official duties.
- I will not attempt to access systems I am not authorized to access.
- I understand that I have no expectation of privacy while using any UABHS information system resources and that all my activities are subject to monitoring.
- I understand that while using UABHS information system resources I represent the UAB Health System and will conduct business in a professional manner.

**Passwords & Other Access Control Measures:**

- I will utilize passwords that are at least eight characters long and use a combination of letters (upper- and lower-case), numbers, and special characters. If the technology does not support such password complexity, I will use the strongest supported password.
- I will protect passwords and other access information from disclosure. I will not provide my password to anyone, including system administrators, my supervisor or management and will not store them on or about workstations, laptop computers, or other devices.

- I will not store authentication devices such as smart cards on or about workstations, laptop computers, or other devices and remove them promptly whenever I leave my work area.
- I will promptly change initial/default passwords or whenever the compromise of my password is known or suspected.
- I will not attempt to bypass access control measures.

**Data Protection:**

- I understand that I am responsible to protect sensitive information from disclosure to unauthorized persons (those without a need-to-know) in accordance with applicable UABHS information handling guidelines.
- I will not disable or circumvent UABHS technical security controls such as encryption, anti-virus, firewalls, monitoring and administrative tools.
- I will not transfer sensitive information to an unencrypted or un-approved device.
- I understand that I have a responsibility to close or log off applications after use.
- I will not access, process, or store sensitive information on non-UABHS equipment such as personally-owned computers unless properly authorized to do so.

**Internet & E-mail Use:**

- I understand that my Internet and e-mail is for official use, with only limited personal use allowed.
- I will not use public e-mail, chat or other Internet-based communication systems (e.g. AOL, Gmail, Yahoo, Hotmail, MobileMe) to communicate sensitive information.
- I will not use “peer-to-peer” file sharing, “Internet Cloud”, web proxy or Internet-based backup web sites and will consult with the Office of Information Security for approved methods.
- I will not provide personal or official UABHS information solicited by unknown individuals or suspected phishing e-mail or web sites.
- I will not distribute non-business mass mailings, viral e-mails or other spam to fellow e-mail users.

**Software:**

- I agree to comply with all applicable software licenses and copyrights.
- I will not install non-standard software on UABHS equipment without prior approval from Health System Information Services (HSIS). This includes software available for download from the Internet, the UAB campus web site, and personally-owned software.

**Use of UABHS Equipment:**

- I understand that UABHS equipment is to be used for official UAB Health System use, with only limited/incidental personal use as approved by my supervisor on the condition that it does not interfere with my job, deny others access to UABHS information systems, consume significant information system resources, and does not result in significant cost, legal or regulatory risk to UABHS. Examples of unacceptable use include, processing pornography, large personal video/audio/photo libraries, copyright infringements, etc.

**Laptop Computers & Portable Devices:**

- I understand that my UABHS BlackBerry, PDA, or other portable device must be password-protected and/or encrypted using HSIS-approved encryption methods.
- I will not disable any UABHS software or security controls unless I am directed to do so by a UABHS system administrator.
- I will not photograph patients or fellow employees without obtaining proper written consent. I understand that such activities require specific documentation and/or approval.

## Wireless Networking:

- New wireless systems used for UABHS business must be approved by the UABHS Chief Information Officer (CIO).
- Wireless systems not compliant with minimum security controls or UABHS Office of Information Security recommendations are subject to immediate disabling and confiscation of hardware.
- Requests for connectivity to wireless networks shall be approved by the UABHS Office of Information Security.
- UABHS employees are prohibited from the use of guest/public wireless systems for business/patient care.

**Telecommuting (travel, home or satellite office):**

- At my alternate workplace, I will follow the same security policies as those required of me at UAB.
- I will properly dispose of media containing sensitive information in accordance to UABHS policy and procedure.

**Incident Reporting:**

- I will report IT security incidents to the UABHS Office of Information Security as soon as I become aware of the incident.

**Contacting the UABHS Office of Information Security:**

- The UABHS Office of Information Security can be reached by e-mail at infosec@uabmc.edu. Security-related services, self-help resources and information is available on the UABHS internal website at: http://www.oneuabmedicine.org by clicking on "**For Faculty & Staff**" then,"**Information Security**".

## Acknowledgment Statement

I acknowledge that I have read the UABHS Rules of Behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules as well as any applicable UAB policies, standards, procedures, security controls or regulations could result in disciplinary action against me including verbal or written warnings, removal of system access, reassignment to other duties, termination, and criminal or civil prosecution.

☐ **Employee or** ☐ **OTHER** (*Please indicate the status of the undersigned*)

Name (printed): _____

Phone Number: _____

Work E-mail Address: _____

Company/Organization: _____

UAB Department: _____

Location or Address: _____

_____

**Electronic Signature Recorded by HealthStream**

_____ _____

User's Signature Date