POLICY GUIDELINE

Southwest General
Partnering with University Hospitals

650 – Access to Information Systems

Effective Date: 7/25/2016
Revision Dates: 6/2018

Purpose:

Define procedures to request access to Southwest General (SWG) information systems. Adherence to this policy ensures the timely availability of information systems to authorized workforce members.

Policy Statement:

Workforce members are granted access privileges to information systems based on their job duties and responsibilities. This is known as "role-based access."

This access applies the "minimum necessary" and "need to know" principles. Being authorized to view or use a system does not imply access to all the information within that application or system, nor does it imply ownership.

To meet compliance and regulatory standards a completed *System Access Form* is required prior to granting access to a new user or modifying existing user access. The *System Access Form* represents the authorization to establish, modify, or terminate a user's access rights therefore the System Administrator is not permitted to fulfill the request without the completed form.

A user may be required to receive training before obtaining access to an application or system. Such prerequisites are determined by the System Administrator.

Management may limit, suspend, or terminate anyone's access privileges at any time.

Definition of Terms:

Confidential information includes, but is not limited to:

- Information about a patient, also known as protected health information (PHI), including incident reports and patient outcome information
- Social Security numbers (patients, employees, and other individuals)
- Credit cards, cardholder information, and bank account numbers
- Business and proprietary information including, but not limited to, patient service methods, costs, pricing, such business matters as contracts, negotiations, strategies, marketing plans, financial statements and other financial information, and legal matters
- Personnel records relating to an employee or medical staff
- Passwords and access codes

Data Owners (aka Information Owners) - the person responsible for (or dependent upon) the business process associated with an information asset. Owners usually are at a Director level or higher.

Information systems – An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and data.

ISSO – Information System Security Officer

System Administrator – Each application system is to have a designated System Administrator. Depending on the application, the System Administrator may be an associate from the application's primary user department or it may be a member of IT. The System Administrator provides general administrative functions, user guidance, and first level support for the application.

Users – Workforce members and associates with authorization to use (access) SWG's computer systems and applications.

Workforce (workers) – Includes employees, trainees, contractors, and individuals who have an association with SWG to perform services and/or have access to SWG data.

Resources: The Information Security Officer should be contacted by the Department Manager/Director for interpretations, resolution of problem and any special situations.

Policy Authority:

- Mary Ann Freas, Sr. VP, CFO, CIO

References:

- HIPAA Security Rule: §164.308(a)(3)(ii)(C), §164.308(a)(4)(i), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), and §164.308(a)(5)(i)
- PCI Data Security Standard: 7.1 and 7.2

Related (Supporting) Policies:

- Policy No. 203 Electronic Email and Fax Usage
- Policy No. 206 Internet Access
- Policy No, 207 Information Technology (IT) Systems Evaluation and Approval
- Policy No. 501 Corrective Action
- Policy No. 617 Computer Software and Hardware Licensing

Implementation Procedures:

Request and Authorization

The appropriate HR personnel, supervisor, or manager completes the *System Access Form* to request and authorize a user's access to information systems. This form can found on the Intranet under "IT Requests, System Access Requests, Download System Access Form." Only those individuals who are authorized to access a system will have the application installed on their workstation. Each individual has a separate security clearance within the application.

The *System Access Form* should be filled out at least 5 working days prior to the new user's start date, whenever possible, to allow the System Administrators sufficient time to set up the new user and create the proper security profiles in each system. System Administrators are not permitted to fulfill the request without the completed System Access form.

Within each application or system, access privileges are normally predefined using role-based access, meaning that access privileges are based upon a user's job function, department, and/or management's authorization.

The System Administrator reserves the right to ensure that:

- Only those who are authorized to access systems are granted access
- Authorized users of an information system have the correct rights and features assigned to them (that are appropriate for their role and security of the SWG network)

For applications or systems that require user training, user access may be established before training by the System Administrator.

Each user will be assigned unique user identification (user ID).

Changes to Access

The appropriate supervisor or manager may request revised access or exceptions to the normal role-based access for a particular user. Revisions or exceptions are requested using the *System Access Form* through the IT Help Desk. The request for access should specify the specific privileges required and, in some cases, may require a justification for the change.

If a user's job duties change, the appropriate supervisor or manager notifies the System Administrator using the *System Access Form* so that the user's access privileges can be matched to their new responsibilities. System Administrators are not permitted to fulfill the request without the completed System Access form.

Monitoring

Access privileges of users are reviewed periodically by the users' supervisor or manager to determine if access still is required and if existing access privileges are appropriate.

Temporarily Suspending or Disabling Accounts

User accounts within Active Directory (AD) that have been inactive for more than 120 days will be reviewed by the IT department and disabled if it is determined that the account is no longer needed. Upon the employee's return, a *System Access Form* will be submitted by their supervisor to re enable the user's access.

Termination of Access

When a user's employment or contract ends, a *System Access Form* is submitted to the IT Help Desk so that the user's access can be disabled, within one business day.

Management has the right to terminate a user's access at any time without warning due to inappropriate use or behavior.

Attachments: See page 5

Applicability: (Select all that apply)

WHO: ☒ Employees ☒ Physicians ☒ Volunteers ☒ Other: Contractors and Business Associates

SITES: ☒ **All Sites** – (if not all, check applicable sites)

☐ Brookpark Urgicare
☐ Brunswick Medical Center
☐ Commerce Park
☐ Health Center Main Campus
☐ Home Health
☐ Hospice
☐ Jefferson Park
☐ Lifeworks
☐ Oakview
☐ Off Campus Business Locations
☐ Southwest General Medical Group Physician Offices
☐ Strongsville Medical Center

☐ Other:

- *System Access Form*

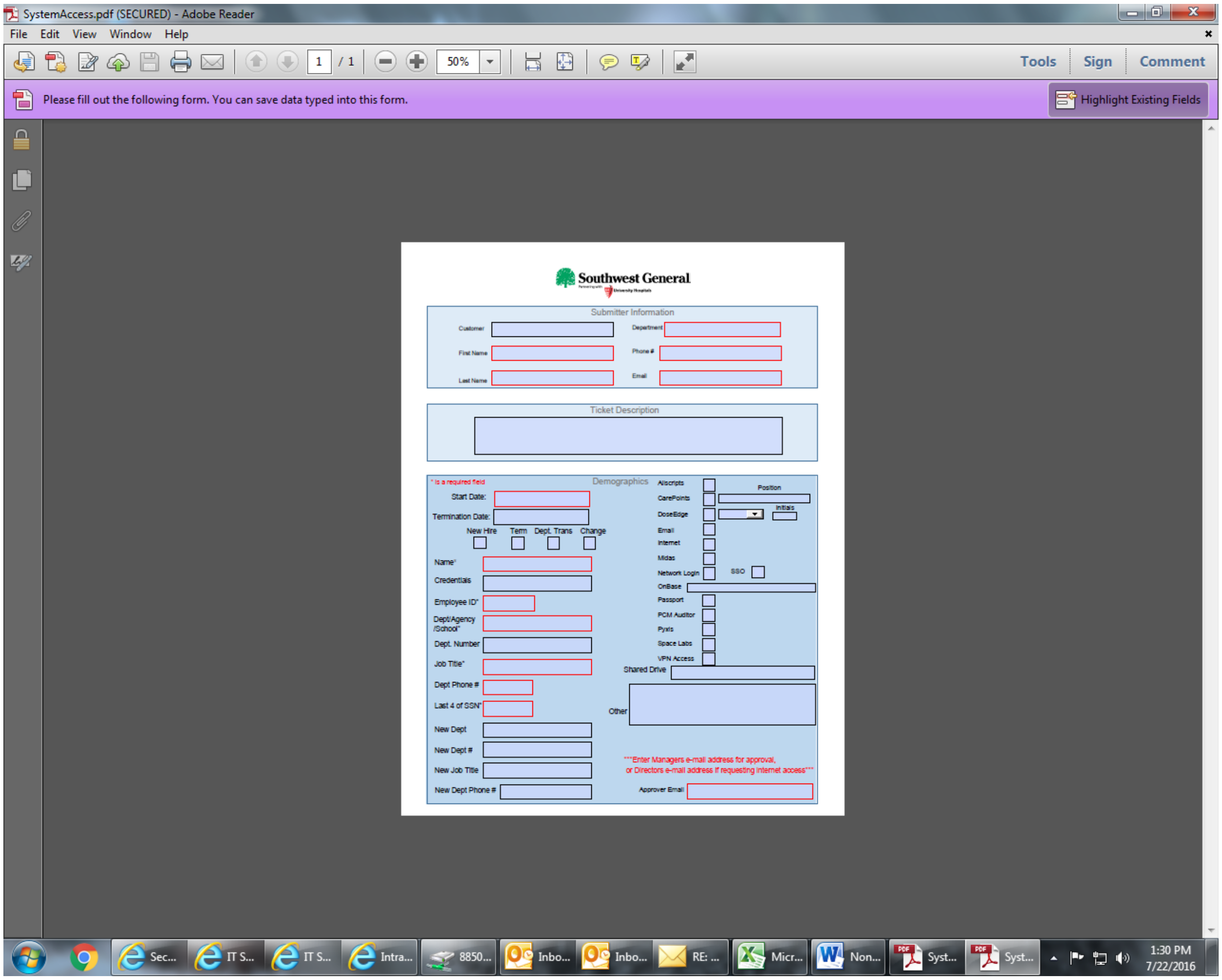
APPROVED:

____

William A. Young, Jr.
President and CEO
Southwest Community Health System

ATTACHMENT A

SYSTEM ACCESS FORM



Please fill out the following form. You can save data typed into this form.

Southwest General
Partnering with University Hospitals

Submitter Information

Customer ______ Department ______
First Name ______ Phone # ______
Last Name ______ Email ______

Ticket Description

______

* Is a required field

Demographics

Start Date: ______
Termination Date: ______
New Hire □ Term □ Dept. Trans □ Change □
Name* ______
Credentials ______
Employee ID* ______
Dept/Agency /School* ______
Dept. Number ______
Job Title* ______
Dept Phone # ______
Last 4 of SSN* ______
New Dept ______
New Dept # ______
New Job Title ______
New Dept Phone # ______

Allscripts □
Position
CarePoints □ ______
Initials
DoseEdge □ ______ ▼ ______
Email □
Internet □
Midas □
Network Login □ SSO □
OnBase ______
Passport □
PCM Auditor □
Pyxis □
Space Labs □
VPN Access □
Shared Drive ______
Other ______

***Enter Managers e-mail address for approval,
or Directors e-mail address if requesting internet access***

Approver Email ______