UNIVERSITY *of* NORTH TEXAS HEALTH SCIENCE CENTER *at Fort Worth*

★

Education, Research, Patient Care *and* Service

USE & TRANSMISSION OF PATIENT INFORMATION USING ONLINE RESOURCES POLICY AND PROCEDURES

MSRDP Operating Procedure Number:	MSRDP 1.003
Effective Date:	May 1, 2001, Revised May 14, 2004
Prepared By:	MSRDP Business Administration
Purpose:	Operating rules for employees who utilize third-party online (World Wide Web) resources to verify patient eligibility, process managed care referrals and/or pre-authorization requests, and check the status of submitted claims.

Approval: _____
Chairman, MSRDP Board of Directors

1.0 **Policy.** Online third party resources will be used to the maximum extent possible to support clinical business operations and improve efficiency. The MSRDP Healthcare Information Systems Analyst and UNTHSC Information Technology Services shall strictly control access to online third party resources. Patient medical information will be safeguarded as prescribed in Federal and State law and UNTHSC policy.

2.0 **Purpose.** To improve efficiency in clinical and business operations while ensuring sensitive patient information is safeguarded consistent with Federal and State laws and UNTHSC policy.

3.0 **Definitions Third Party Online Resources**. Dial-up or World Wide Web (www) sites used by third party entities that allow for the verification of eligibility, processing of specialty referrals and/or precertification requests, and inquiries regarding the status of submitted claims. Examples of these applications are *BlueLINK* (Blue Cross/ Blue Shield of Texas).

4.0 **Procedures** In consultation with the Associate Dean and Chief Medical Officer, the Chief Operating Officer/Executive Director of MSRDP and the Director of Business and Clinical Services will evaluate and authorize the use of third party online resources for UNTHSC clinical departments. This evaluation shall include a review of the prospective payer/vendors operating and security procedures in compliance with Texas Privacy Act & Gramm Leach Bliley Act. Under no circumstances will a payer/vendor be authorized for use by clinical departments if user passwords are shared. Additionally, each payer/vendor is required to accept centralized access termination notice from MSRDP.

4.1 Once authorized, the MSRDP Information Systems & Training Department shall:

4.1.1 Evaluate authorized entity's training program and materials and adapt or integrate those materials as applicable to current MSRDP training courses.

4.1.2 Coordinate and/or conduct training on the authorized entity's online resource.

4.1.3 Document and administer authorized users by clinical department for each entity's online resource. This shall include access termination notification to MSRDP Healthcare Information Systems Analyst and UNTHSC Information Technology Services by the Senior Administrative Official in the clinic or designee within 24 hours of resignation/termination.

4.2 Once authorized, the Senior Administrative Official in each department shall:

4.2.1 Designate in writing to the MSRDP Healthcare Information Systems Analyst and MSRDP Training Department primary and alternate users for each clinic site and coordinate user training at each site.

4.2.2 Ensure that each authorized user safeguards their respective log-in name and password. Under no circumstances will passwords be shared among employees or be displayed adjacent to a personal computer.

4.2.3 Monitor the use of each online resource to determine its usefulness in clinical and business operations and provide periodic feedback, as necessary to the Vice president, Practice Operations and Chief Medical Officer.

4.2.4 Ensure that violations of this policy and procedure are administered in a manner consistent with UNTHSC Human Resource Services policy and procedures.

4.3 Once authorized by the Senior Administrative Official in each department, each employee shall:

4.3.1 Protect all unique passwords for all online third party resources which includes but is not limited to: (1) sharing passwords with co-workers, (2) posting passwords adjacent to computers with access to the online third party resource, (3) logging off online third party resource when all work has been

completed or the computer cannot be visually monitored by the authorized employee, and (4) changing any password that may have become compromised. It is permissible for employees to write their passwords down and place them in a sealed envelope that is in a secured (i.e., department safe) central location with access controlled by the Senior Administrative Official.

4.3.2 Ensure that online third party resources are only accessed using UNTHSC computer resources during normal business hours and days. The Senior Administrative Official in each department can authorize their employees access to these systems in conjunction with approved overtime requests.

4.4 Failure to comply with MSRDP Policy and Procedure or UNTHSC Computer Resources Security Policy may result in immediate progressive disciplinary action that include, but may not be limited to:

- Oral warning
- Formal written reprimand
- Suspension without pay
- Termination of employment
- Civil prosecution, or
- State and/or federal criminal prosecution

4.5 Access to on-line electronically transmitted health information is to be restricted:

- To 'normal' business hours and days
- Utilized for official state purposes only
- To use by authorized individuals
- Access to, changes to, and uses of must be strictly secured

5.0 **References :** UNTHSC Computer Resources Security Policy
The State of Texas Penal Code, Chapter 33 (Texas Computer Crimes Statute)

6.0 **Follow-Up and Review** This policy and procedure shall be reviewed every year.

7.0 **Responsibility** Senior Associate Dean and Chief Medical Officer
Vice President, Practice Operations and Chief Administrative Officer
MSRDP Healthcare Information Systems Analyst
UNTHSC ITS LAN Analyst
Senior Administrative Official in each Patient Care department