

# INTER-INSTITUTIONAL INFORMATION SECURITY AGREEMENT (ISA)

This agreement applies to the employees, temporary employees, physicians, students, faculty, and contract personnel of

Children's Medical Center,  
Parkland Health & Hospital System,  
UT Southwestern Health Systems,  
UT Southwestern Medical Center,  
St. Paul University Hospital, and  
Zale Lipshy University Hospital

hereafter referred to as "Participating Institutions". Your signature is maintained as part of the information security program. If you do not accept this agreement, access to Participating Institutions' systems will be immediately denied.

It is the policy of the Participating Institutions to protect all information resource assets. Information resources refers to all hardware and software, and any format of available or recorded patient information or state information whether automated, hardcopy, fax, e-mail, etc. Information security policies and guidelines, as established by the Participating Institutions, apply to all information that is recorded, transmitted, stored, and/or processed manually or by a computer system, when the protection of that information is deemed essential. These security policies and guidelines also apply to information resources owned by others, in those cases where the Participating Institutions have a contractual or fiduciary duty to protect the resources while in custody of the Participating Institutions.

All information resources under management by Participating Institutions are strategic and vital assets, and require a degree of protection commensurate with their value. Measures shall be taken to protect these assets against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity and availability of information.

1. Access to, and use of, information resources is restricted to appropriately identified, validated, and authorized users.
2. All means of access to automated information resources, such as user access codes and passwords, are confidential and proprietary to the Participating Institutions. Information resources include, but are not limited to, network systems and applications; mainframe, midrange, and PC applications; and voice mail or long distance telephone codes. Holders of such access means are accountable for their unauthorized or negligent disclosure or use. Providing assigned user-IDs or passwords to unauthorized personnel is a violation of the Texas Penal Code.
3. State law requires that information resources be used only for official purposes.
4. Proprietary software may not be copied in violation of a licensing agreement. In cases involving multiple use of a single product, e.g., in networks, software must be used in accordance with the license agreement.
5. Risks to information resources must be managed at all levels. Access to and/or modification of, information that is confidential, sensitive, and/or essential to critical functions must conform to security policy procedures and standards.
6. On termination of employment, contractual relationship, or cessation of student enrollment with any of the Participating Institutions, or as otherwise requested by appropriate management, users must surrender all property and information managed by the Participating Institution, and must not subsequently disclose any confidential or sensitive information. Access to information resources will cease at this time.

# INTER-INSTITUTIONAL INFORMATION SECURITY AGREEMENT (ISA)

## VIOLATIONS OF POLICY

In the event any person violates these policies, access rights will be immediately revoked and the individual will be subject to immediate disciplinary action, which may include suspension without pay, expulsion, or termination of employment or contract. In accordance with section 3.6 of the Regents Rules and Regulations, students can be assessed penalties ranging from disciplinary probation up to and including expulsion from the institution. In addition, the individual may be subject to civil or criminal legal sanctions when a violation occurs.

Suspected or confirmed violations of these policies should be reported to appropriate management. Use the numbers below to obtain a copy of your institution's individual guidelines:

**Children's Medical Center**, contact the Director of Information Services at (214) 456-6126

**Parkland Health & Hospital System**, contact the Chief Information Security Officer at (214) 590- 5999

**UT Southwestern Health Systems**, contact the Director of Information Systems at (214) 645-0314

**UT Southwestern Medical Center**, contact the Information Security Officer at (214) 648-1300

**St. Paul University Hospital and Zale Lipshy University Hospital**, contact the Director of Information Systems at (214) 590-9333

## CLINICAL DATA

Clinical data contains patient information that is highly sensitive. This sensitive information when viewed either electronically or hardcopy version should never be discussed outside the clinical environment in support of the patient's care. Each time you electronically view patient information, an audit trail may be created which includes your identification code, dates and times of access, and your location. This audit trail is in compliance with the Participating Institutions' strong commitment toward patient confidentiality and security.

Reports can be generated at any time that reflects your activities. A patient can request a report of all users who have viewed their record. Authorized personnel review these reports. If inappropriate actions are suspected, a memo and copies of these reports will be sent to the appropriate personnel. For Medical and Allied Health students, this information will be sent to their respective Associate Dean for Student Affairs. For Graduate students, this information will be referred to the Dean of the Graduate School. For all other users, this information will be sent to the supervisor, department chair, legal services, and/or Human Resources.

All electronic patient information should remain confidential in the same way and to the extent required by law that paper medical record information is confidential. Printing, copying and distribution of electronic patient information should be made only by authorized persons in the Medical Records Departments authorized to provide such disclosure.

# INTER-INSTITUTIONAL INFORMATION SECURITY AGREEMENT (ISA)

## ACKNOWLEDGEMENT

*I acknowledge that I have received the Information Security Agreement (ISA). I have read the ISA and understand that I must comply with it when accessing and using information resources. My failure to comply with the ISA may result in cancellation of my privilege of use, appropriate disciplinary action, and action by law enforcement authorities.*

*By signing this notification, I also indicate my understanding of my personal responsibilities in maintaining a patient's right to privacy. I agree that I will only access information of the patients for which I am directly providing or supporting the clinical care.*

SIGNATURE		
PRINTED NAME (Last, First, Middle Initial)		
TODAY'S DATE	PERSON # OR EMPLOYEE #	
SOCIAL SECURITY NUMBER*	CAMPUS PHONE NUMBER	
CHECK PRIMARY INSTITUTION OF EMPLOYMENT		
<input type="checkbox"/> CMC <input type="checkbox"/> PHHS <input type="checkbox"/> UTSHS <input type="checkbox"/> UTSW <input type="checkbox"/> ZLUH <input type="checkbox"/> SPUH		
DEPARTMENT	SUPERVISOR	SUPERVISOR'S PHONE #
CHECK APPROPRIATE STATUS		
<input type="checkbox"/> Full-time Employee <input type="checkbox"/> Part-time Employee <input type="checkbox"/> Temporary Employee <input type="checkbox"/> Faculty <input type="checkbox"/> Volunteer Faculty		
<input type="checkbox"/> Fellow <input type="checkbox"/> Student <input type="checkbox"/> _____		

### UTSW/ZLUH/SPUH

For faster service please FAX signed form to 214-648-6656. Mail original to UT Southwestern Systems Account Management (SAM), Mail Code 9084.

Information Security and Patient Confidentiality Who, What, and Where Video viewed: Y  N

### PARKLAND

Fax signed form to 214-590-0222. Mail original to Parkland InfoSec Dept., Bank One Suite 500.

\*Non-UT Southwestern employees are required to supply only the last four digits of their SSN.