



Workers Compensation Data Confidentiality Agreement

I. This paragraph constitutes information security training for the purposes of this document.

Electronic data maintained by the State Office of Risk Management and stored on the mainframe computer at the Office of the Attorney General is sensitive information. It must be given a reasonable degree of protection to ensure that only individuals who specifically need to work with it can have access to it. Your access to this information will be controlled by means of a User Name and a Password. Both will be unique to you. You will be required to change your password periodically. Your User Name will remain the same as long you require access to this data and will be inactivated when your need for access ends. It is vital that you keep your User Name and Password secure. Do not share them with anyone. Do not write them down and leave them where there is even a slight possibility they will be found. If you forget your Password, SORM can easily reset it.

The same security principles apply to the information itself as well. Do not access information you don't need to see. Take precautions to insure that information you have in your possession stays among people who have a reason to see it. Do not access information dealing with any case involving yourself or any of your relatives, friends or business associates.

In summation, any information obtained about employees is strictly confidential; any disclosure of this information is a violation of SORM policy and may be a violation of state or federal law. Information obtained about individual workers compensation claims is for the official use of Texas state agencies and should not be disclosed to anyone else, including the injured employee. Any inquiry from an injured employee should be directed to the SORM adjuster handling the case.

II. By signing this statement, I certify that I:

- Agree to abide by all written information security policies imposed by SORM
- Understand the following responsibilities as a user of SORM information resources
 1. Use the resources only for the purpose specified by its owner
 2. Comply with controls established by the owner
 3. Prevent disclosure of confidential information
- Am not permitted to access information on, or in any way deal with, any case involving myself, or any of my relatives, friends or business associates
- Have received the User's Manual for the Claims Management System and will comply with the procedures established
- Notify SORM of any change in my email address
- Notify SORM of any change in my employment status which would result in my no longer requiring access to this

My failure to comply with the information security policies of SORM may result in denial of my access, **or my agency's access**, to the data concerned, as well as possible disciplinary actions within my own agency. Failure to observe the above conditions or any attempt to circumvent the computer security by using or attempting to use any transaction, software, files, resources, or passwords that I am not authorized to use may constitute a "Breach of Computer Security" as defined in the TEXAS PENAL CODE, Chapter 33, Section 33.02, B, and that such an offense is a Class A Misdemeanor. Similar federal statutes may also be applicable. Copies of the TEXAS PENAL CODE, Chapter 33, Section 33.02 are available from the Information Security Officer.

The following should be filled out and signed by the person requesting access and authorized by the agency's designated Primary Claims Coordinator.

User Information

Agency Name:

Agency Number:

Location Code:

Name of Person Requesting Access:

Title/Function:

Email Address:

SSN:

Phone:

Requestor's Signature: _____

Date: _____

Primary Claims Coordinator or Authorized Representative

Name (Please Print): _____

Title: _____

Signature: _____

Date: _____

Please fax the completed form to Will Boiney at (512) 370-9194.
(Be sure to include all 3 pages.)