

- I. PURPOSE:** To establish policy, procedures and responsibility for the security and sharing of the personal information of members, employees, and those contracted to provide services, hereafter referred to as sensitive information.
- II. POLICY:**
- A. Sensitive information shall be confidential. This includes information in or accessed from the following media: paper, personal computers, Facsimile machines, PBX systems, Internet or other electronic equipment (e.g. Palm Pilots).
 - B. Sensitive information shall not be given, made available, or disclosed to any individual, corporation, institution, organization, agency or government agent, hereafter all referred to in total as organizations, without written informed consent of the involved party or a valid court order or subpoena, issued by a court of competent jurisdiction.
 - C. Access without written informed consent to sensitive information shall be limited to the Board of Directors, hereafter referred to as the BOD, employees, and committee chairs with a bona fide need to know. The President, with approval of the BOD, has the authority to grant or remove this access.
 - D. WSTRA shall annually request, in writing, informed consent to share specific sensitive information with organizations, including, but not limited to, members, TR-related organizations, and non-TR related organizations.
 - E. All sensitive information, regardless of the method of storage, shall be maintained against physical and/or electronic intrusion.
- III. PROCEDURE:**
- A. Sensitive information maintained may include, but is not limited to:
 - 1. Name
 - 2. NCTRC Certification Number
 - 3. Membership Category
 - 4. Employer
 - 5. Position
 - 6. Population Working With
 - 7. Mailing Address, City, State, Zip
 - 8. Home Telephone
 - 9. Business Telephone
 - 10. Fax Telephone
 - 11. E-mail Address
 - 12. WSTRA Payments
 - 13. WSTRA Educational Opportunities Attended
 - 14. WSTRA Products Purchased
 - 15. WSTRA Committee Membership
 - 16. Professional Recognition Earned
 - B. Distribution of sensitive information with written informed consent must be approved by a quorum majority of the WSTRA Board of Directors.
 - C. Written informed consent to share specific sensitive information is obtained either on the membership application form or by separate informed consent.
 - 1. Name, employer, position, population, mailing address, city, state, zip, telephones, e-mail address, and membership category can be shared with any organizations

approved by the BOD unless otherwise specified in writing. A statement regarding this will be prominently displayed in the membership application and contracts.

2. Members, employees and those contracted to provide services may refuse consent to share sensitive information, except in case of valid court order or subpoena, issued by a court of competent jurisdiction. This opportunity will be included in the membership application and contracts.
3. Separate informed consent will be obtained for non-recurring sensitive information sharing.

D. Recurring Sensitive Information Sharing

1. The sharing of sensitive information is event specific. Sensitive information is useable only for the event requested and is not allowed for use for future events.
2. A Membership Directory is published and distributed annually to members. It includes sensitive information of current members not refusing consent.

Information may include, and is limited to the following:

- a. Name
- b. Membership Category
- c. Current Employer, Position, and Population Working With
- d. Mailing Address, City, State, Zip
- e. Home Telephone
- f. Business Telephone
- g. Fax Telephone
- h. E-mail Address
- i. Current WSTRA Committee Membership
- m. Professional Recognition Earned

3. Mailing Labels

- a. Sensitive information of members shared on mailing labels may include, and is limited to:
 - (1) Name
 - (2) Membership Category
 - (3) Mailing Address, City, State, and Zip.
- b. The BOD determines the member benefit and fees charged at the time of information sharing approval.
- c. Labels are given free-of-charge to BOD approved TR-related organizations for TR-related educational or research purposes of direct benefit to the majority of members.
- d. Labels are given for a fee to BOD approved TR-related organizations for TR-related purposes not of direct benefit to the majority of members. The fee will not exceed the actual cost of the labels + mailing costs + cost of personnel time + 10%.
- e. Labels are given for a fee to BOD approved nonTR-related organizations for purposes of benefit to the majority of members. The fee will not be less than the actual cost of the labels + mailing costs, + cost of personnel time + 25%.

- E. Firewall software and/or hardware protects sensitive information stored on an electronic device accessing a LAN, WAN or the Internet. Sensitive information stored on paper will be protected by lock.

- F. Backup of all data stored electronically is performed each time data is updated. Backup media is stored separate from the electronic location to protect from disaster occurring at the electronic location.
- G. Upon presentation of a court order or subpoena to the President or designated authority of WSTRA, the BOD and all employees and members subject to such documents will delay its enforcement until such time as the BOD consults with legal counsel to determine that such document is a valid order.
- H. Disposal of sensitive information is done by shredding or similar means of protecting confidentiality and security.

IV. RESPONSIBILITY:

- A. All Association personnel
 - 1. Maintain the confidentiality and security of sensitive information.
 - 2. Will not share the Membership Directory with non-association personnel or organizations.
- B. Board of Directors
 - 1. Approve organizations that may be given sensitive information with written informed consent to distribute.
 - 2. Determine fees for the sharing of sensitive information as appropriate.
 - 3. Consultation with legal counsel in case of presentation of a court order or subpoena.
- C. President or designee
 - 1. Grant or remove access, without the written informed consent of the affected party, to sensitive information.
 - 2. Ensure adequate safeguards are in place to protect sensitive information security.
 - 3. Evaluate sensitive information security at least every two years.
 - 4. Review, investigate and implement corrective action for sensitive information security violations.
 - 5. Publish a statement regarding the sharing of sensitive information on contracts.
 - 6. Publish a method to refuse the sharing of sensitive information on contracts.
 - 7. Obtain written informed consent for non-recurring sensitive information sharing.
- D. Secretary and Membership Committee Chair or designees
 - 1. Collect, verify accuracy, maintain and protect needed sensitive information.
 - 2. Publish a statement regarding the sharing of sensitive information on the membership application.
 - 3. Publish a method to refuse the sharing of sensitive information on the membership application.
 - 4. Publish, maintain accuracy and ensure allowable distribution of an annual Membership Directory. Ensure inclusion of only allowable sensitive information of current members not refusing consent.
 - 5. Publish and ensure accuracy of mailing labels. Ensure inclusion of only allowable sensitive information of current members not refusing consent.
 - 6. Protect sensitive information, stored on an electronic device accessing a LAN, WAN or the Internet, by a software and/or hardware firewall.
 - 7. Backup electronically stored data. Store backup media and paper reports appropriately.

- E. Organizations receiving sensitive information with written informed consent to be shared:
 - 1. Will not copy, scan or other save shared sensitive information.
 - 2. Use shared sensitive information only for the one event requested. Will not use shared sensitive information for any event not specifically requested.

V. REFERENCES:

- A. American Therapeutic Recreation Association policy regarding confidentiality.
- B. National Certification of Therapeutic Recreation Council policy regarding confidentiality.

VI. RESCIND: Information Security and Sharing, expiration September, 2004.

VII. EXPIRATION DATE: November, 2008. Reviewed biannually or as determined by the BOD.

VIII. FOLLOW-UP RESPONSIBILITY: WSTRA President

Chrystal Smith, CTRS/R
President, WSTRA, April 2004 – April 2005