Texas State Guard

INSTRUCTION

TXSGI 8000-10
20 MAY 2021
NGTX-XHZ

SUBJECT: Safeguarding Protected Health Information (PHI) and Sensitive Personal Information (SPI)

References. (a) Texas Medical Privacy Act (Tex. Health & Safety Code § 181.001, et seq.), which incorporates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191).
(b) Identity Theft Enforcement and Protection Act (Tex. Bus. & Comm. Code § 521.001, et seq.)

1. PURPOSE. This instruction provides guidance and instruction for the maintenance and protection of PHI and SPI and requirements for training of individuals accessing or managing PHI and SPI.

2. APPLICABILITY AND SCOPE. This issuance applies to all TXSG personnel reviewing, accessing, or managing PHI and SPI.

3. DEFINITIONS.

a. **Breach of System Security**. Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

b. **Individually Identifiable Health Information**. Information relating to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual and that identifies or could identify the individual. This type of information includes:

(1) Names;

(2) Addresses;

(3) Birthdates, treatment dates, discharge and admission dates, and ages;

(4) Telephone numbers;

(5) Fax numbers;

(6) Email addresses;

(7) Social security numbers;

(8) Medical record numbers;

(9) Health plan beneficiary numbers;

(10) Account numbers;

(11) Certificate/license numbers;

(12) Vehicle identifiers, including license plate numbers;

(13) Device identifiers and serial numbers;

(14) URLs;

(15) IP addresses;

(16) Biometric identifiers, including finger and voice prints;

(17) Full face photographic images and any comparable images; and

(18) any other unique identifying number, characteristic, or code.

c. Personal Identifying Information. information that alone or in conjunction with other information identifies an individual, including an individual's:

(1) name, social security number, date of birth, or government-issued identification number;

(2) mother's maiden name;

(3) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(4) unique electronic identification number, address, or routing code; and

(5) telecommunication access device.

d. Sensitive Personal Information.

(1) an individual's first name or first initial and last name in combination with any one or more of the following items:

(a) social security number;

(b) driver's license number or government-issued identification number; or

(c) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(2) information that identifies an individual and relates to:

(a) the physical or mental health or condition of the individual;

(b) the provision of health care to the individual; or

(c) payment for the provision of health care to the individual.

(3) The term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government

e. **Victim.** A person whose identifying information is used by an unauthorized person.

4. POLICY. This instruction supports directives described in JFTX Reg 1-01, Safeguarding Personally Identifying Information (PII).

a. While the TXSG is not a covered entity under HIPAA, a covered entity under the Texas Medical Privacy Act must comply with HIPAA's provisions. As a potentially covered entity under the Texas Medical Privacy Act, the TXSG must comply with HIPAA's requirements as to protection of individually identifiable health information and the disclosure of PHI.

(1) PHI, including individually identifiable health information, may only be disclosed with permission of the individual.

(2) Any PHI, including any individually identifiable health information, should be maintained in a confidential manner and should not be disclosed, forwarded, or used in any manner other than necessary for treatment and/or evaluation. When in doubt as to whether something is protected or within a permitted use, keep the information as private and confidential as possible, and if it needs to be disclosed, seek authorization to do so.

(3) PHI, including any individually identifiable health information, should not be disclosed in response to any Open Records Request.

b. All members will receive training regarding the state and federal law concerning PHI as necessary and appropriate for the members to carry out their duties. This training must be completed within 90 days of assumption of duties and documented with a signed certificate of training.

c. Individual medical providers serving in the Medical Brigade are responsible under their applicable license for complying with their applicable confidentiality requirements under Texas and federal law. Their responsibilities under their license for patient confidentiality do not change when they provide health care as a member of the TXSG.

d. SPI of individuals must be protected and disposed of in a manner to keep the information from being stolen or used.

e. A victim must be notified if their SPI is accessed by a breach of system security as quickly as possible.

f. No TXSG service member or civilian employee may obtain, possess, transfer, or use PHI, including individually identifying health information, SPI, or personal identifying information of another member or any other person outside the course and scope of the individual's duties within the TXSG.

g. Records not maintained by the TXSG containing SPI or PHI including individually identifying health information, must be destroyed by shredding, erasing, or otherwise rendering any SPI or PHI, including individually identifying health information, unreadable or indecipherable.

5. RESPONSIBILITIES. All TXSG leaders will ensure this guidance is disseminated throughout their units, understood, enforced, and followed by their personnel.

6. INFORMATION REQUIREMENTS. NA.

7. RELEASABILITY. Unlimited.

8. EFFECTIVE DATE. This instruction will expire 2 years from the effective date of publication unless sooner rescinded or superseded.

9. POINT OF CONTACT. T1, TXSG 512-782-6223.

ROBERT J. BODISCH, SR.
Major General, TXSG
Commander

DISTRIBUTION:
A