97406 Data Security Standards for Standardized Limited Datasets and Other Confidential Data

(a)

The following definitions apply to this section: (1) "NIST" is the National Institute of Standards and Technology, an agency of the United States of America. (2) "FIPS 140 Validation" means current validation by the NIST's Cryptographic Module Validation Program. (3) "FIPS 200" means the Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," dated March 2006, which is hereby incorporated by reference. (4) "Information system" means an applicant's discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of confidential data. (5) "NIST 800-53" means the NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," dated September 2020; and NIST Special Publication 800-53B, "Control Baselines for Information Systems and Organizations," dated October 2020, both of which are hereby incorporated by reference. (6) "NIST 800-88" means Section 5 and Appendix A of the NIST Special Publication 800-88, Revision 1, "Guidelines for Media Sanitization," dated December 2014, which are hereby incorporated by reference.

(1)

"NIST" is the National Institute of Standards and Technology, an agency of the United

States of America.

(2)

"FIPS 140 Validation" means current validation by the NIST's Cryptographic Module Validation Program.

(3)

"FIPS 200" means the Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," dated March 2006, which is hereby incorporated by reference.

(4)

"Information system" means an applicant's discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of confidential data.

(5)

"NIST 800-53" means the NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," dated September 2020; and NIST Special Publication 800-53B, "Control Baselines for Information Systems and Organizations," dated October 2020, both of which are hereby incorporated by reference.

(6)

"NIST 800-88" means Section 5 and Appendix A of the NIST Special Publication 800-88, Revision 1, "Guidelines for Media Sanitization," dated December 2014, which are hereby incorporated by reference.

(b)

All data applicants for confidential data must meet the following requirements: (1) Anyone accessing confidential data shall receive training on information privacy and data security no less than once per year for the duration of their access to confidential data. (2) All software, information systems, computers, and other devices that are used to access confidential data, including through the enclave, shall have security patches applied in a reasonable time. (3) Passwords to access confidential data shall, at a minimum, have 16 characters with at least one capital letter, one small letter, one number, and one special character. (4) All information systems, computers, and other devices that are used to access confidential data, including through the enclave, shall have active antivirus controls. Applicants must provide the security antivirus controls in place by product name and current version.

(1)

Anyone accessing confidential data shall receive training on information privacy and data security no less than once per year for the duration of their access to confidential data.

(2)

All software, information systems, computers, and other devices that are used to access confidential data, including through the enclave, shall have security patches applied in a reasonable time.

(3)

Passwords to access confidential data shall, at a minimum, have 16 characters with at least one capital letter, one small letter, one number, and one special character.

(4)

All information systems, computers, and other devices that are used to access confidential data, including through the enclave, shall have active antivirus controls. Applicants must provide the security antivirus controls in place by product name and current version.

(c)

For direct transmission of confidential data under Section 97396, 97398, or 97400, a data applicant must provide a level of data security for confidential data that is not less than the level required by FIPS 200 and NIST 800-53 for information that is categorized as moderate-impact for the security objective of confidentiality.

(d)

Notwithstanding the above, applicants applying for direct transmission of confidential data under Section 97396, 97398 or 97400 shall comply with the following security requirements: (1) Applicants shall conduct a thorough background check of each individual who will observe, use, or control confidential data on their behalf before the individual has the ability to observe, use, or control the data. This background check shall, at the least, include the individual's history of data breaches, and criminal convictions or substantiated violations of law regarding fraud, theft, data breach, data misuse or related offenses. Based on the thorough background check, applicants shall evaluate whether the individual presents an unreasonable risk of causing a data breach, stealing confidential data, or misusing confidential data and prohibit those who present such a risk from having the ability to observe, use, or control the data. Applicants shall document each background check and evaluation and retain these records for a period of three (3) years after the applicant stops using the confidential data. (2) All computers containing confidential data shall have full disk encryption using modules with FIPS 140 validation. (3) All removable media devices containing confidential data shall be encrypted with software that has FIPS 140 validation. (4) If the Department approves transmittal of confidential data outside of the applicant, the following is required:(A) all electronic transmissions of confidential data outside the information system shall be encrypted using software that has FIPS 140 validation; (B) all mailings of unencrypted confidential data, including hardcopies, shall be sealed, and secured from view by unauthorized individuals and shall be mailed using a tracked mailing method, which includes verification of delivery and receipt. (5) Unencrypted confidential data, including hard copies, shall be stored, and used within applicant's work offices, and when unattended, shall be stored in secured areas with controlled access procedures, where it is not viewable from the outside, and is under 24-hour guard or monitored alarm. (6) Direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations shall be stored separately from other confidential data. (7) Regarding media sanitization, hard copy and digital media with confidential data shall be disposed of as described in NIST 800-88. (8) The applicant must use signature based and non-signature based malicious code protection mechanisms at system entry and exit points.

(1)

Applicants shall conduct a thorough background check of each individual who will observe, use, or control confidential data on their behalf before the individual has the ability to observe, use, or control the data. This background check shall, at the least, include the individual's history of data breaches, and criminal convictions or substantiated violations of law regarding fraud, theft, data breach, data misuse or related offenses. Based on the thorough background check, applicants shall evaluate whether the individual presents an unreasonable risk of causing a data breach, stealing confidential data, or misusing confidential data and prohibit those who present such a risk from having the ability to observe, use, or control the data. Applicants shall document each background check and evaluation and retain these records for a period of three (3) years after the applicant stops using the confidential data.

(2)

All computers containing confidential data shall have full disk encryption using modules with FIPS 140 validation.

(3)

All removable media devices containing confidential data shall be encrypted with software that has FIPS 140 validation.

(4)

If the Department approves transmittal of confidential data outside of the applicant, the following is required:(A) all electronic transmissions of confidential data outside the information system shall be encrypted using software that has FIPS 140 validation; (B) all mailings of unencrypted confidential data, including hardcopies, shall be sealed, and secured from view by unauthorized individuals and shall be mailed using a tracked mailing method, which includes verification of delivery and receipt.

(A)

all electronic transmissions of confidential data outside the information system shall be encrypted using software that has FIPS 140 validation;

(B)

all mailings of unencrypted confidential data, including hardcopies, shall be sealed, and secured from view by unauthorized individuals and shall be mailed using a tracked mailing method, which includes verification of delivery and receipt.

(5)

Unencrypted confidential data, including hard copies, shall be stored, and used within applicant's work offices, and when unattended, shall be stored in secured areas with controlled access procedures, where it is not viewable from the outside, and is under 24-hour guard or monitored alarm.

(6)

Direct personal identifiers listed in Section 164.514(e) of Title 45 of the Code of Federal Regulations shall be stored separately from other confidential data.

(7)

Regarding media sanitization, hard copy and digital media with confidential data shall be disposed of as described in NIST 800-88.

(8)

The applicant must use signature based and non-signature based malicious code protection mechanisms at system entry and exit points.

(e)

If applicants cannot meet a security requirement in subsection (d), they may request exceptions to the requirement in their data application to the Department. The Department shall only grant an exception if it determines that the applicant has adequate alternatives.