PART 324—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

Authority: 5 U.S.C. 301; 40 U.S.C. 121(c)(2).

Source: 80 FR 72151, Nov. 18, 2015, unless otherwise noted.

Subpart 324.1—Protection of Individual Privacy

324.103 Procedures for the Privacy Act.

324.104 Restrictions on Contractor Access to Government or Third Party Information.

324.105 Contract clauses.

Subpart 324.70—Health Insurance Portability and Accountability Act of 1996

324.7000 Scope of subpart.

324.7001 Policy on Compliance with HIPAA business associate contract requirements.

Parent topic: SUBCHAPTER D—SOCIOECONOMIC PROGRAMS

Subpart 324.1—Protection of Individual Privacy

324.103 Procedures for the Privacy Act.

(a) The contracting officer shall review all acquisition request documentation to determine whether the requirements of the Privacy Act of 1974 (5 U.S.C. 552a) are applicable. The Privacy Act requirements apply when a contract or order requires the contractor to design, develop, or operate any Privacy Act system of records on individuals to accomplish an agency function. When applicable, the contracting officer shall include the two Privacy Act clauses required by Federal Acquisition Regulation (FAR) 24.104 in the solicitation and contract or order. In addition, the contracting officer shall include the two FAR Privacy Act clauses, and other pertinent information specified in this subpart, in any modification which results in the Privacy Act requirements becoming applicable to a contract or order.

(b) The contracting officer shall ensure that the statement of work or performance work statement (SOW or PWS) specifies the system(s) of records or proposed system(s) of records to which the Privacy Act and the implementing regulations are applicable or may be applicable. The contracting officer shall send the contractor a copy of 45 CFR part 5b, which includes the rules of conduct and other Privacy Act requirements.

(c) The contracting officer shall ensure that the contract SOW or PWS specifies for both the Privacy Act and the Federal Records Act the disposition to be made of the system(s) of records upon completion of contract performance. The contract SOW or PWS may require the contractor to destroy the records, remove personal identifiers, or turn the records over to the contracting officer. If there is a legitimate need for a contractor to keep copies of the records after completion of a

contract, the contractor must take measures, as approved by the contracting officer, to keep the records confidential and protect the individuals' privacy.

(d) For any acquisition subject to Privacy Act requirements, the requiring activity prior to award shall prepare and have published in the Federal Register a “system notice,” describing the Department of Health and Human Services' (HHS) intent to establish a new system of records on individuals, to make modifications to an existing system, or to disclose information in regard to an existing system. The requiring activity shall attach a copy of the system notice to the acquisition plan or other acquisition request documentation. If a system notice is not attached, the contracting officer shall inquire about its status and shall obtain a copy from the requiring activity for inclusion in the contract file. If a notice for the system of records has not been published in the Federal Register, the contracting officer may proceed with the acquisition but shall not award the contract until the system notice is published and the contracting officer verifies its publication.

324.104 Restrictions on Contractor Access to Government or Third Party Information.

The contracting officer shall establish the restrictions that govern the contractor employees' access to Government or third party information in order to protect the information from unauthorized use or disclosure.

324.105 Contract clauses.

(a) The contracting officer shall insert the clause at 352.224-70, Privacy Act, in solicitations, contracts, and orders that require the design, development, or operation of a system of records to notify the contractor that it and its employees are subject to criminal penalties for violations of the Privacy Act (5 U.S.C. 552a(i)) to the same extent as HHS employees. The clause also requires the contractor to ensure each of its employees knows the prescribed rules of conduct in 45 CFR part 5b and each contractor employee is aware that he or she is subject to criminal penalties for violations of the Privacy Act. These requirements also apply to all subcontracts awarded under the contract or order that require the design, development, or operation of a system of records.

(b) The contracting officer shall insert the clause at 352.224-71, Confidential Information, in solicitations, contracts, and orders that require access to Government or to third party information.

Subpart 324.70—Health Insurance Portability and Accountability Act of 1996

324.7000 Scope of subpart.

All individually identifiable health information that is Protected Health Information (PHI), as defined in 45 CFR 160.103 shall be administered in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) implementing regulations at 45 CFR parts 160 and 164 (the HIPAA Privacy, Security, and Breach Notification Rules). The term “HIPAA” is used in this part to refer to title II, subtitle F of the HIPAA statute, at part C of title XI of the Social Security Act, 42

U.S.C. 1320d *et seq.,* section 264 of HIPAA, subtitle D of title XIII of the American Recovery and Reinvestment Act of 2009, and regulations under such provisions.

324.7001 Policy on Compliance with HIPAA business associate contract requirements.

(a) HHS is a HIPAA “covered entity” that is a “hybrid entity” as these terms are defined at sections 160.103 and 164.103 respectively. As such, only the portions of HHS that the Secretary has designated as “health care components” (HCC) as defined at section 164.103, are subject to HIPAA. HHS' HCCs may utilize persons or entities known as “business associates,” as defined at section 160.103. Generally, “business associate” means a “person” as defined by section 160.103 (including contractors, and third-party vendors, etc.) if or when the person or entity:

(1) Creates, receives, maintains, or transmits “protected health information”, as the term is defined at section 160.103, on behalf of an HHS HCC to carry out HHS HIPAA “covered functions” as that term is defined at 164.103; or

(2) Provides certain services to an HHS HCC that involve PHI.

(b) Where the Department as a covered entity is required by 45 CFR 164.502(e)

(1) and 164.504(e) and, if applicable, sections 164.308(b)(3) and 164.314(a), to enter into a HIPAA business associate contract, the relevant HCC contracting officer, acting on behalf of the Department, shall ensure that such contract meets the requirements at section 164.504(e)(2) and, if applicable, section 164.314(a)(2).