<?xml encoding="UTF-8">

1239.7101 Definitions.

As used in this subpart—

Breach means the disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized access, compromise, use, disclosure, modification, destruction, access or loss use of data, or the copying of information to unauthorized media may have occurred.

Data protection means the practice of protecting data and managing risks associated with the collection, display, use, processing, storage, transmission, and disposal of information or data as well as the systems and processes used for those purposes. Data protection uses physical, technical, and administrative controls to protect the integrity, availability, authenticity, non-repudiation, and confidentiality of data by incorporating protection, detection, and reaction capabilities. Data protection encompasses not only digital data, but also data in analog or physical form, and applies to data in transit as well as data at rest.

Information security means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) *Integrity,* which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(2) *Confidentiality,* which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) *Availability,* which means ensuring timely and reliable access to and use of information.

Personally Identifiable Information (PII) means the definition as set forth in FAR 24.101.

Privacy incident means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access to PII regardless of format.

Parent topic: Subpart 1239.71—Protection of Data About Individuals