Since the data of which we are speaking belongs to the Dept of Education, it is subject to the controls and directives under which the Department must operate. One source of these directives is the Office of Management and Budget (OMB), who in January of 2017 issued directive M-17-12 : "Preparing for and Responding to a Breach of Personally Identifiable Information." This directive contains the following language (p. 9):

Definition of an Incident:
An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Definition of a Breach:
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PU by means of a network intrusion, a targeted attack that exploits website vulnerabilities,or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PU and portable electronic storage media that store PU, the inadvertent disclosure of PU on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for an other than authorized purpose. Often,an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PU, as is often the case with a lost or stolen laptop or electronic storage device.

Some common examples of a breach include:
• A laptop or portable storage device storing PU is lost or stolen;
• An email containing PU is inadvertently sent to the wrong person;
• A box of documents with PU is lost or stolen during shipping
• An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;
• A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;
• An IT system that maintains PII is accessed by a malicious actor; or
• PII that should not be widely disseminated is posted inadvertently on a public website.