DITA Topic Map

Contents

Data Visibilities

All raw data and derived data stored in the PHEMI system can be tagged with attributes that provide information about the data's sensitivity and the visibility it should have to different system users. These attributes are called data visibilities.

The visibilities you define for your data should reflect the sensitivity of the data as identified by your organization. The PHEMI system predefines three visibilities pertaining to privacy:

Table 1: System-Defined Data Visibilities

Visibility	Description
IDENTIFIED	Sensitive data that contains identifying information. Such data should be secured and available only to authorized personnel.
DE_IDENTIFIED	Sensitive data that has been transformed and masked to remove identifying information
NONIDENTIFIED	Data that does not contain sensitive or identifying data.

You can define additional data visibilities to suit your organization's needs. Possible examples are CONFIDENTIAL to identify data that is sensitive and requires a user to a certain level of access or certification to access, PII to identify Personally Identifiable Information, PHI to identify personal health information, or SECRET to identify especially sensitive material.

Note: Once defined, a data visibility may be neither edited nor deleted.

The data visibilities specified for a data source are referred to in *access policies* and matched against user *authorizations* to determine what actions, if any, a given user is allowed to perform on the data.

Any data visibility defined in the system can be used by a Data Processing Function (DPF) to tag data elements, or cells, derived by the DPF. For example, the Social Security Number extracted from a health record can be tagged CONFIDENTIAL if that data visibility has been defined in the system. This mechanism provides "cell-level" privacy protection.