NetIQ® Identity Manager™

Driver for Epic Implementation Guide

July 2021

Legal Notices

Contents

Understanding the Epic EMP Driver (Overview) 5

1 Driver Features 9

Supported Operations 9
Entitlement Support 10
Special Attribute Handling 10

2 Installing the Epic Driver 13

System Requirements 13
Driver Dependencies 13
Security Recommendations 13
Driver Packages 13
Installing the Driver Files 14
Extending Schema For Supporting Custom Attributes 15
Creating the Driver Object 15
Importing the Current Driver Packages 15
Activating the Driver 16
Authentication 16
Driver Parameters 16
Global Configuration Values 17

A Appendix - Troubleshooting the Driver 21

B Appendix - Driver Schema to Epic EMP Number Mapping 23

C Appendix - Primary Manager 25

D Definitions, Acronyms, and Abbreviations 27

Understanding the Epic EMP Driver (Overview)

Epic is an Electronic Medical Records (EMR) management system that maintains medical records and provides providers and patients with access to said medical records. Epic is one of the leading EMR systems in use throughout the healthcare industry. Epic contains PHI and PII and is therefore required to meet HIPAA regulatory requirements.

Driver Concepts

The Identity Manager (IDM) Driver for Epic EMP is a connector that allows for identity life cycle management of Epic EMP (login account) records. Within the Epic EMR ecosystem there are 2 main record types; EMP and SER; this driver manages EMP records only. The driver works on the Subscriber channel only, as Epic currently does not have an event system or a full database query facility.

Epic does not utilize groups as part of its architecture. Instead, Epic utilizes the concept of security templates to assign access within the application. The Epic EMP driver takes advantage of this architecture and allows the assignment of these templates and sub-templates within Epic via the assignment of IDM entitlements. A user may only be assigned a single template, but sub-templates may be assigned to the user to supplement their security access within the Epic system.

Data Transfer Between Systems

The Epic driver communicates with Epic using the Epic SOAP APIs.

In order to use the Epic driver, the Epic Interconnect Web Services must be licensed and enabled within the Epic system. Contact the Epic administrator for help enabling this service.

Publisher Channel

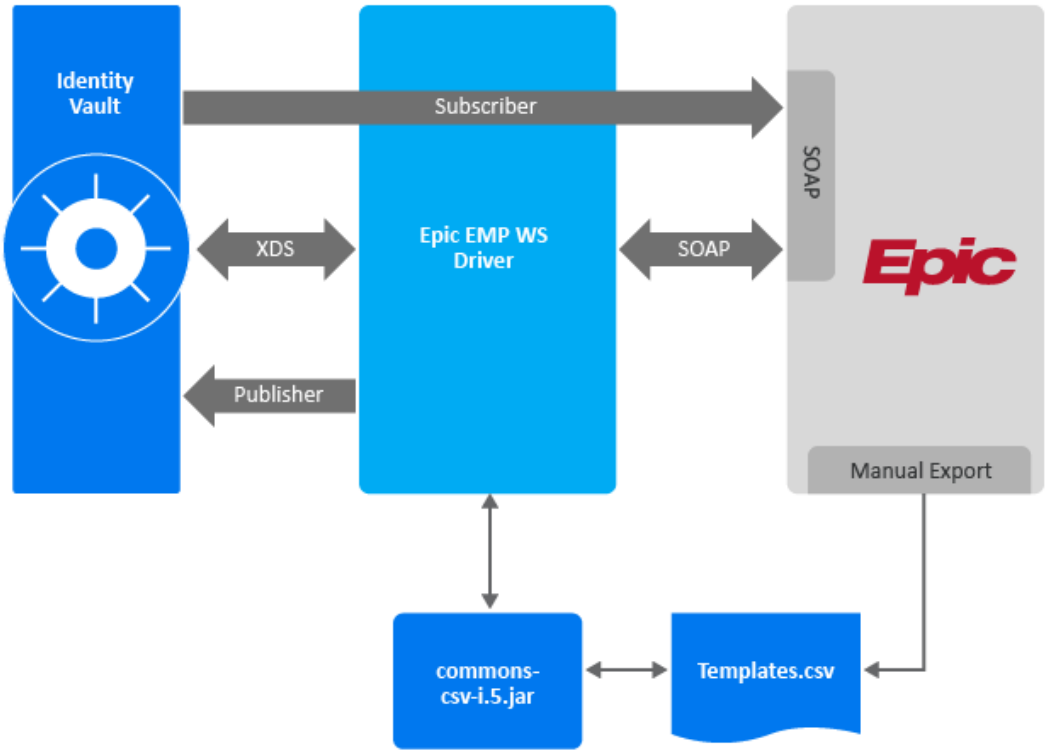
The publisher channel is not currently supported on this driver.

Subscriber Channel

The driver synchronizes the User class from the Identity Vault to Epic (on the subscriber channel). Attributes synchronized are specific to each individual implementation but typically contain the CN, jobCode, Login Disabled, naming attributes, and other user level attributes.

How the Driver Works

The Epic EMP driver shim is a java shim that establishes a SOAP connection to the Epic EMP interface. Epic EMP records are updated via this connection.



The CSV file containing the linkable templates and sub-templates should be provided by your Epic security team and updated regularly. The CSV format is as follows:

```
ID,DESC,TYPE
T00239,ABSTRACTION SUBTEMPLATE,Subtemplate
TACCESS,ACCESS PROJECT TEAM,Linkable Template
ADMIN,"ADMIN, EPIC",Linkable Template
T3102601,ADT ADMIT SUPERVISOR TEMPLATE,Linkable Template
```

Standard Use Cases

The following is a list of standard use cases and benefits for the Epic EMP driver:

- Automatic user account creation in Epic.
- Automatic updates in Epic on managed accounts and attributes.
- Mapping of Epic security template assignment to job or business roles in IDM.
- Security templates may be assigned via policy on the Epic EMP driver subscriber channel.
- Security templates may be assigned via role and resources in IDM Dash.
- Security templates may be assigned via role and resources via Identity Governance business roles or technical roles.
- Re-evaluate Epic security when job roles change within the organization.

- Enforce least level of security within Epic.
- Management of external account assignments within Epic.

1 Driver Features

Supported Operations

- Add Operations
  - Add operations are supported
- Modify Operations
  - Add Value is supported
  - Remove Value is not supported

    NOTE: The Epic APIs do not support removing a specific value from an attribute. All attribute values must first be removed and then the attribute must be reset. Because of this API restriction, the driver shim will return a message of `Remove-Value not supported`. Appending `add-value` elements when a `remove-value` operation is submitted.
  - Remove All Values is supported
- Delete Operations
  - Delete operations are supported
- Rename Operations
  - Rename operations are supported
- Move Operations
  - Move operations are supported
- Query Operations
  - The following query operations and classes are supported:
    - User class
      - Only supported for `systemLoginID`, `userInternalID`, and `externalID` attributes in Epic.
    - LinkableTemplate class
      - Only supported for Code Map Refresh events
      - Query executes against template CSV file identified in driver configuration
    - UserSubtemplate class
      - Only supported for Code Map Refresh events
      - Query executes against template CSV file identified in driver configuration
  - `<query-ex>` operations are not supported
- Modify Password Operations
  - Modify Password operations are not supported

- Check Object Password Operations
  - Check Object Password Operations are not supported
- External IDs and Passwords
  - Epic has the concept of an External ID(s) and Password(s). The driver does support External IDs and Passwords.

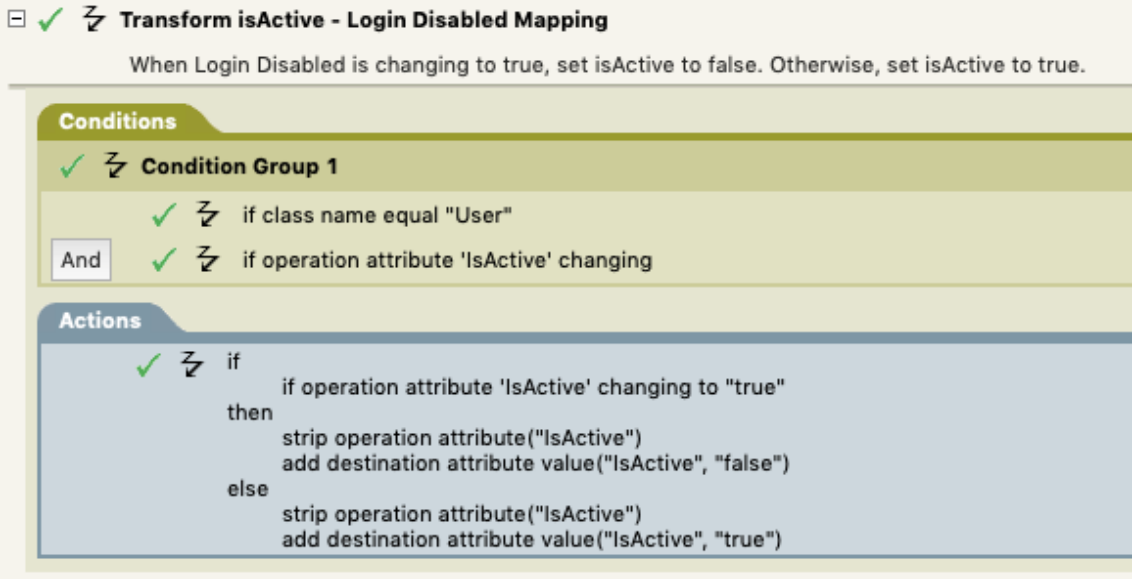
Entitlement Support

The driver supports entitlements for linkable templates and sub-templates in Epic. This is accomplished by exporting, from Epic, the linkable templates and sub-templates to a CSV file. For more information, see "How the Driver Works" on page 6.

When a code map refresh is issued by the driver the resulting query for linkable templates and sub-templates is routed by the driver shim through the `commons-csv-1.8.jar` where the previously exported `templates.csv` file is read, and the response is returned to IDM with the entitlement values.

Special Attribute Handling

Login Disabled: When mapping Login Disabled in the Identity Vault to IsActive in Epic the value must be reversed for the desired outcome. When Login Disabled is set to true in the Identity Vault the matching result in Epic for IsActive would be false. If the attribute us synced straight through without changing the value, the result will be the opposite of what is desired.



CustomUserDictionaries: This attribute is an indexed array of strings in Epic. To set the order of the values beings sent to Epic, an optional XML attribute `order` can be used. The lowest order number is 1. If no order is provided the driver will auto increment and the order of the values will not be guaranteed.

```
<modify-attr attr-name="CustomUserDictionaries">
    <remove-all-values/>
    <add-value>
        <value order="2" timestamp="1530022566#6" type="string">Users\Dict
ionaries\Shared-dictionary.tlx</value>
    </add-value>
    <add-value>
        <value order="1" timestamp="1530022566#6" type="string">Users\Dict
ionaries\Bobs-dictionary.tlx</value>
    </add-value>
</modify-attr>
```

2 Installing the Epic Driver

System Requirements

The Epic EMP driver requires a minimum version of Identity Manager 4.7. If entitlements are being used, then IDM 4.7 Advanced Edition or newer is required.

The Epic EMP driver will run on the IDM engine or on a remote loader.

Driver Dependencies

- Apache Commons CSV 1.8 (`commons-csv-1.8.jar`) – This is used for reading the linkable templates and sub-templates. This file is available in the extracted driver zip folder **> windows**.
- URL of SOAP Endpoint – WSDL location can be URI format (https://server/path/epic.wsdl) or a file path (file:/var/opt/epic/epic.wsdl)
- CSV containing the linkable templates and sub-templates. This list should be provided by the Epic security team and updated regularly.

Security Recommendations

- The Epic EMP driver must have the ability to read objects and attributes listed in driver subscriber filter in addition to standard Identity Manager driver security requirements
  - For more information on object synchronization, see Synchronizing Objects in the *NetIQ Identity Manager Driver Administration Guide*.
- Epic's SOAP interface is accessible over HTTPS. The Epic EMP driver must be able to connect to the Epic SOAP interface over this https connection. Make certain any firewall rules are updated to allow the Epic driver to communicate with Epic (TCP port 443 unless otherwise configured in the Epic implementation).
- Audit User in Epic – The identifier of the person who is creating the new User record. Epic generally recommends that this field be left blank, although some implementations will require a value.
- Epic Client ID – Starting with the February 2019 Epic build all API calls must have a Client ID. There are options on how to implement this; the Epic Driver is using the http header option.

  For more information, see "Activating the Driver" on page 16.
- Trust all Certs – Though it is not recommended, if the Epic system is utilizing a self-signed certificate, the "Trust All Certs" driver configuration may be enabled (there are security risks associated with utilizing this functionality as it can potentially open the system to MIM attacks).

Driver Packages

The following packages are utilized by the driver:

Package Name	Min Version	Link	Notes on how it is being used
Epic EMP Driver	2.0		This is the driver base package
Epic EMP Driver Default	2.0		This package provides the default configuration parameters and policies
Epic EMP Driver Entitlements	2.0		This package provides support for driver entitlements to include Entitlement objects, GCVs, Driver Policies, and Driver Resources
Advanced Java Class (NOVLLIBAJC)	2.2		ECMAscript functions are used by the driver policies

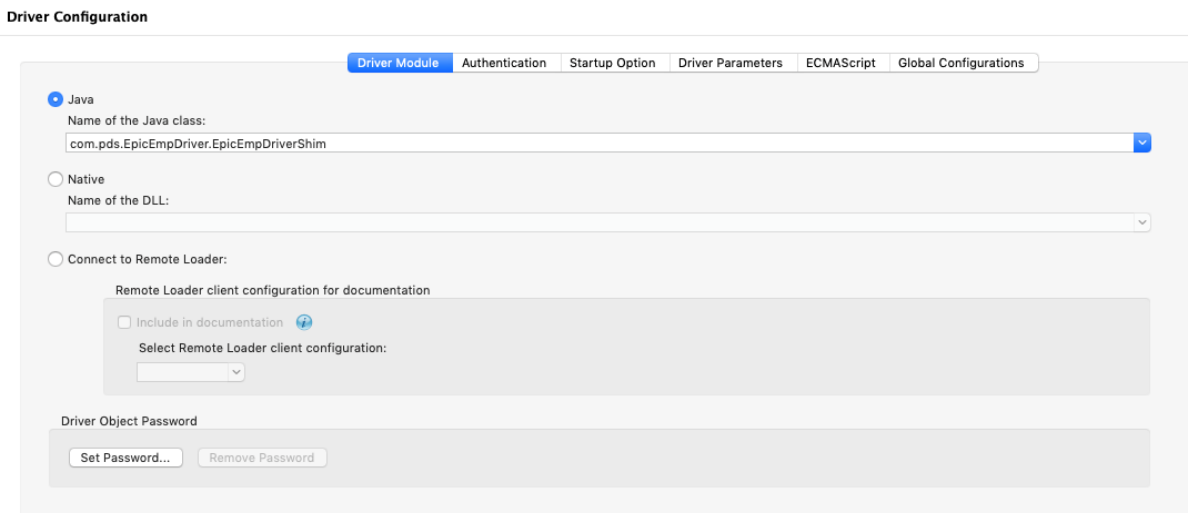
Installing the Driver Files

To install the driver files you must perform one of the following actions based on your platform:

- **Linux**:
  1. Navigate to the extracted driver zip folder **> linux**.
  2. Install the `netiq-DXMLEpicEMP.rpm` in your driver installation directory by running the following command in a terminal window.

     `rpm -Ivh <rpm file path>/netiq-DXMLEpicEMP.rpm`
  3. Restart Identity Vault.
- **Windows**:
  1. Navigate to the extracted driver zip folder **> windows**.
  2. Copy the `EpicEmpDriver.jar` file and the `commons-csv-1.8.jar` into the `/opt/novell/eDirectory/lib/dirxml/classes` directory, or `\Novell\RemoteLoader\lib` if the driver is installed with the Remote Loader.
  3. Restart Identity Vault.

When creating the Designer driver object the name of the Java class is: `com.pds.EpicEmpDriver.EpicEmpDriverShim` as shown in the following image.



Extending Schema For Supporting Custom Attributes

You can upload new attributes through the Identity Manager to extend the schema. The following steps explain the procedure to extend the schema:

1. Navigate to the extracted driver zip folder **> schema.**
2. Copy the `epicID.sch` file to the system where Identity Manager is installed.
3. Execute the following `ndssch` command.

   ```
   ndssch [-h hostname[:port]] [-t tree_name] [-d] admin_FDN schemafile [schema_description]
   ```

   For example, `ndssch -h 10.71.131.123:524 -t SLES12SP3_Quality_131123_TREE -d admin.sa.system /root/schema/epicID.sch`
4. The log file is created in the default location, `/root/schema.log` for troubleshooting.
5. Restart Identity Manager to see the schema changes.

Creating the Driver Object

To create the Epic EMP driver the driver packages must first be installed in the Designer project's **Package Catalog**. When creating the driver object, these packages must be added to the driver object and configured for the target environment.

Importing the Current Driver Packages

To import the driver packages into Designer please use the following steps:

1. Open Designer.
2. In the Outline view, right-click the **Package Catalog**.
3. Click **Import Package**.
4. Browse to the location where the *Epic EMP Driver*, *Epic EMP Driver Default*, and *Epic EMP Driver Entitlements* packages were downloaded.

5. Select all packages for the *Epic EMP Driver*.
6. Click **Select All** to import all of the packages displayed in the screen.
7. Click **OK** to import the selected packages, then click **OK** in the successfully imported packages message.
8. After the packages are imported the driver object may be created and configured for the target environment.

Activating the Driver

The Epic EMP driver is activated by loading the Epic EMP Driver Micro Focus license key.

Note that the driver must be activated within 90 days of installation, else the driver stops working and an activation error will be displayed in the driver trace file.

Additionally, the driver must also be registered with Epic for use in the customer's Epic environments. This is done in 1 of 3 manners:

- The customer's App Orchard Point Person (AOPP) contacts their Epic App Orchard TS and provides the application name of "Micro Focus IDM Driver for User Management".
- The customer registers the driver with Epic by submitting the App Orchard App Request Process document located on Epic's Galaxy documentation portal.
- The customer contacts their Micro Focus Account Executive who could have the driver registered on the customer's behalf.

Authentication

Parameter	Description
Authentication ID	The authentication ID for the driver. The format is `EMP:<ID>`
Set Password	The password for the driver

Driver Parameters

The following driver parameters are set for the Epic EMP driver

Driver Options

Parameter	Description
Epic Version	The version of the Epic implementation. Select 2017 if the implementation is running Epic 2017 or newer
Epic Environment	Select Production or Non-Production
ID Types	A list of custom ID types (Item 20700/20701) to set. This is very implementation specific. When an ID type is added here it will show in the Schema as `IDType-<value>`. The value listed here comes from the `ID type descriptor` under **Names in Other Systems** in the ID type definition in Epic. **NOTE:** In the ID Type definition under the ID Rules tab in Epic the **Method** must be **either user entered or system generated**.
Trust All Certs	If enabled, tells the driver to trust all certs when establishing the https connection to the Epic SOAP endpoint (there are security risks associated with utilizing this functionality as it can potentially open the system to MIM attacks)

Subscriber Options

Parameter	Description
URL of SOAP Endpoint	The WSDL location for the Epic SOAP endpoint. This can be of either, file or URI format (that is, https://server/path/epic.wsdl or file:/var/opt/epic/epic.wsdl)
Enable Data Courier Log File	Yes or No as to enable the data courier log file
Path for data courier log files	The location to store log files if enabled
Force Contact on all Updates	Yes or No as to force **contact** on updates in Epic. If set to yes, the Epic will create a new contact record on every update from the driver.
Audit User	The audit user in Epic that will be identified as the creator of a new User record
Audit User Password	The audit user's password
Path to template CSV file	The full file path to the location of the template CSV file provided by Epic for linkable templates and sub-templates

Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

Configuration

The following driver parameters are set for the Epic EMP Driver Default package.

Parameter	Description
Use Epic ID for Create	◆ If **true** selected, then the value of the user's configured *Epic ID* attribute will be used when creating the EMP record. Note that if there is: ◆ no *Epic ID* value set on the user, then the create will be vetoed. ◆ If **false** is selected, then *Epic ID* will arbitrarily assign the ID on create of EMP record.
Epic ID Attribute	Attribute in IDV containing Epic ID value to use during EMP record creation.

Entitlements

The following driver parameters are set for the Epic EMP Driver Entitlements package.

Parameter	Description
Use User Account Entitlement	When the driver is enabled for entitlements, accounts are only created and removed/disabled when the account entitlement is granted to or revoked from users. Entitlements are granted and revoked only by entitlement agents. Three entitlement agents ship with Identity Manager: ◆ **Role-Based Entitlements (RBE)**: RBE is ideal for simple automation. For example, when a user is added to the HR system, the user is automatically granted accounts in other systems ◆ **Workflow**: Workflow is ideal for approvals. For example, when a user is added to the HR system, the manager must approve the accounts for the user. ◆ **Roles Based Provisioning Module (RBPM)**: RBPM is ideal for true and full-featured roles based provisioning. For example, when a user is added to the Accounting role, the user automatically receives all accounts associated with the Accounting role. If **True** is selected, one of these entitlement agents must be installed and configured for the driver to create and delete accounts. For more information, see the Identity Manager Entitlements Guide.
Enable Login Disabled attribute sync	Select whether the changes made to the **Login Disabled** attribute in Identity Vault should be synced even if the User Account entitlement (UserAccount) is enabled.
When account entitlement revoked	Choose what action is taken in Epic when a User Account Entitlement is revoked; **Disable Account** or **Block Account**.
Block Comment	A freetext comment to send with the event, about why the User is blocked. The maximum length is 100 characters.
Enable External Identifier Entitlement	Select **Yes** to enable the management of External Identifiers via driver entitlements.

Parameter	Description
Enable Standard Template Entitlements	Select **Yes** to enable the standard management of Templates via driver Available Template, Default Template, and Applied Template entitlements.

A Appendix - Troubleshooting the Driver

Driver is not starting or connecting to Epic

- Validate that the WSDL address entered in the Subscriber Settings is correct
- Validate that the firewall ports are open to allow access Epic
- Validate that the Authentication ID is in the format `EMP:<ID>` (i.e. `EMP:BSMITH`)
- Ensure that the driver is fully activated. For more information, see “Activating the Driver” on page 16.

User update is failing

- If a user record is locked (i.e. open in Epic Hyperspace) the driver will not be able to update the user. There is an error reported in the driver trace.
- Is there a policy trying to do a *remove value* instead of a *remove all values*? Remove value operations are not supported on the driver, *remove all values* must be used.

Error “INVALID-CLIENT-ID details: Provided client ID is invalid” in trace

- Ensure that the driver is fully activated. For more information, see “Activating the Driver” on page 16.

B Appendix - Driver Schema to Epic EMP Number Mapping

The following table details the supported Epic schema and the driver schema to Epic EMP Number mapping:

Driver Schema	EMP Number
userInternalID	.1
name	.2
systemLoginID	45
startDate	720
endDate	730
userAlias	180
reportGrouper1	280
reportGrouper2	281
reportGrouper3	282
categoryReportGrouper1	283
categoryReportGrouper2	284
categoryReportGrouper3	285
categoryReportGrouper4	286
categoryReportGrouper5	287
categoryReportGrouper6	288
primaryManager	20414
defaultLoginDepartmentID	20660
customUserDictionaries	17460
identityTypes (IDType-*xxxxx*)	20700/20701

C Appendix - Primary Manager

Using the Epic driver, one cannot just assign any user as a manager. There are certain conditions that must be met to assign a user as a manager. These conditions are listed below:

- The manager must have their ID listed in the Users Managers List
- The target manager has to have an `InBasketClassification` that has In Basket security point `14-Manage Clinic` or `16-Trusted Manager`.
- If the value of the user's manager attribute has an association ref (dn reference) the association value is used otherwise the value is used. `<value association-ref="113" timestamp="1530022566#6" type="dn">\MMEYER_IDV47_TREE\data\users\PDSTester2</value>` or `<value timestamp="1530022566#6" type="dn">FAMMD</value>`.

NOTE: The value used must be the `epicID` of the target manager.

D Definitions, Acronyms, and Abbreviations

The following key terms are used in conjunction with the Epic EMP driver:

- Contact - point and time version of the EMP record
- Data Courier - Data courier logs are used to move configuration changes between different Epic environments
- EMR – Electronic Medical Records
- EMP Record – User Login Record in the Epic system
- External ID - Value of a user name external to the Epic system
- HIPAA - Health Information Portability and Accountability Act
- IDM - Identity Manager
- Item – Attribute of an EMP record
- Linked (Linkable) Template – Grouping of items to be applied to EMP record (often security related)
- PII – Personally Identifiable Information
- PHI – Personal Healthcare Information
- SER - Schedulable Epic Resource