Identity Assurance Level (IAL) Assessment Worksheet

General Information	
System Name: *Enter the name of the system for which the IAL Assessment is being completed.*	ACME Partner Portal.
System Description: *Enter a brief but adequate description of the system. The description should provide a summary of what the system is, its purpose, whom it serves, etc.*	*ACME Partner Portal provides access to Medicaid treatment records for patients (PHI) that can be sorted by age, resident geographic area and treatment codes. Users are able to perform queries, view results, perform analysis and generate reports. Reports can be saved by screen shot or downloaded as a PDF file. Some users with the Analyst 2 role can view and save reports containing PHI.*
Government Interaction Supported: *Check the appropriate box(es) that best indicate(s) the type of government interaction the system supports:* • *Government-to-Citizen – Interaction between state government and its citizens.* • *Government-to-Business – Interaction between state government and the private business sector.* • *Government-to Government – Interaction across all levels of government (federal, state, local, tribal).*	☐ Government-to-Citizen X Government-to-Business ☐ Government-to-Government
Date Assessment Completed: *Enter the date on which the IAL Assessment was completed.*	3/28/15
Information Owner: *Enter the name and the functional title of the Information Owner for the information associated with this system, along with his or her contact information. The Information Owner is the person in the State Entity responsible and accountable for the security of the information. Information owners are typically at the manager or executive level.* ***Note:*** *Information owners are typically not IT personnel. IT personnel only implement the security controls set forth by the information owner to protect the confidentiality, integrity, and availability of the information asset.*	Name: William Smith Functional Title / Job Title: CIO ACME Hospital Association Phone #: Email:

IAL Assessment Team Members: *Enter the names of the IAL Assessment Team, their functional job title, and their contact information, starting with the IAL Assessment Team chair or leader.*	**IAL Assessment Team Chair/Team Leader** Name: Jane Doe1 Functional Title: Patient Data Attorney Phone #: Email: **IAL Assessment Team Members** Name: Susan Smith Functional Title: CISO, ACME Hospital Association Phone #: Email: Name: John Doe3 Functional Title: Deputy COO Phone #: Email: Name: Mary Williams Functional Title: ACME PPS Business Analyst Phone #: Email: Name: Functional Title: Phone #: Email:

IDENTIFY USER TYPES

In this section, identify the set of users that will have authenticated access to the system.

User Role:

Identify the user types (e.g., citizen, vendor, NYS employee) that will be accessing the system.

User Role Description:

Provide a brief description of the user role.

	User Role	User Role Description
1	*Provider Analyst 1*	*Ability to see patient counts, treatment counts, frequency. No access to ePHI*
2	*Provider Analyst 2*	*Ability to see patient records, treatments, medications and diagnosis codes for individual patients. Access to ePHI. User can produce reports that contain PHI for up to 10,000+ patients at a time.*
3		
4		
5		

Determine Risk and Impact

User Role: Analyst 2

User Role Description: *Ability to see patient records, treatments, medications and diagnosis codes for individual patients. Role permits access to ePHI.*

Enter one user role, and its associated description listed above, for which this table will be completed.

DETERMINE CONSEQUENCES

Consequence Statements: *For each identified transaction, write a consequence statement for each of the six (6) questions, indicating the potential consequences to the State Entity or to the user (enter N/A for a question if not applicable) in the event (of an authentication error) a non-authorized individual were to conduct the transaction.*

There is no need to provide a consequence statement if a question does not apply. Conversely, it is possible to identify many consequences in response to a single question that is particularly relevant to the transaction.

TRANSACTIONS SUPPORTED								
Transaction Name *Provide the transaction's name.*	**Transaction Description** *Provide a description of the transaction. Describe the actions the user can perform using the following action words: inquire, create, modify, delete, approve, or cancel.*	**Data Sensitivity** *Identify the data used in the transaction/system, and specifically note whether the data is restricted to certain actors or groups of actors as it contains sensitive information. Indicate the law or regulation governing the data.*	1. What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?	2. What potential financial losses would be incurred by any involved party?	3. What effect(s) would result from an unauthorized release of sensitive information?	4. To what civil or criminal violations would the agency be subject? (Out of compliance with regulatory rules.)	5. What harm to agency programs or public interest would be realized?	6. How would personal safety be impacted?
Query by County and Diagnosis Code	**Query**- returns # of patients with one or more diagnosed conditions by county. User can also return the actual patients. Each returned record contains Patient name, SSN, sex, DOB, Medicaid ID, diagnosis codes.	Data con contain de-identified data as well as PHI.	Reputation of ACME could be impacted if a breach made it to the press. Patients could be subject to blackmail threats if their data fell into the wrong hands.	Because data is PHI a breach could be subject to an investigation and potential penalty. A HIPAA violation due to reasonable cause and not due to willful neglect. $1,000 per violation, with an annual maximum of $100,000 for repeat violations. $1.5M max per year. This breach of 10,000 records results in $1M fine. ACME would need to provide	ACME subject to penalty. Significant loss of reputation to ACME. ACME would need to report the breach to HHS and it becomes public.	If breach was severe enough there could be civil or criminal actions. If ACME failed to provide necessary protections this could open them up to such actions.	Public loss of trust in ACME, patients may seek treatment elsewhere..	None, data was not modified only leaked.

				notification and credit watch services.				
DETERMINE IMPACT LEVELS *Using the Table titled Identity Assurance Level Required for guidance, assign an impact value (1, 2, 3, 4) to each of the six (6) questions, based on the consequence statements associated with each. If there is more than one transaction for the user, then consider the consequence statement that poses the greatest risk and thus the greatest potential impact to the agency.*	☐ 1 None ☐ 2 Little ☒ 3 Serious/limited ☐ 4 Serious/severe	☐ 1 None/ insignificant ☐ 2 Minor ☒ 3 Serious ☐ 4 Severe/catastrophic	☐ 1 None ☐ 2 Limited ☒ 3 Serious ☐ 4 Catastrophic	☐ 1 None ☐ 2 No enforcement ☒ 3 Possible enforcement ☐ 4 Enforcement	☐ 1 None ☒ 2 Limited ☐ 3 Serious ☐ 4 Severe or higher	☒ 1 None ☐ 2 Minor ☐ 3 Non-serious ☐ 4 Serious/Death

Identity Assurance Level Required

For each of the six (6) category questions, check the corresponding impact level in the matrix below, using the highest impacted user role per each consequence statement as identified in the Determine Risk and Impact table above. (Note: A box can be checked by double-clicking on the appropriate box and selecting "Checked" and "OK" from the pop-up.)

Category of Harm	Identity Assurance Impact Levels			
1. What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?	☐ **1** **No** inconvenience, distress or damage to the standing or reputation of any party	☐ **2** **Little** inconvenience, distress or damage to the standing or reputation of any party	☒ **3** A **serious short-term or a limited long-term** inconvenience, distress or damage to the standing or reputation of any party	☐ **4** A **serious or severe long-term** inconvenience, distress or damage to the standing or reputation of any party
2. What potential financial losses would be incurred by any involved party? **Note:** The severity of the loss depends on the impact of the loss on the affected party	☐ **1** **No or insignificant/in-consequential** unrecoverable financial loss to any party or an insignificant/incons equential agency liability	☐ **2** A **minor** unrecoverable financial loss to any party or a minor agency liability	☒ **3** A **serious** unrecoverable financial loss to any party or a serious agency liability	☐ **4** A **severe or catastrophic** unrecoverable financial loss to any party or a server or catastrophic agency liability
3. What effect(s) would result from an unauthorized release of sensitive information? **NOTE:** The severity of the effect is due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal, government or commercial information	☐ **1** **No loss or adverse effect** on an individual or agency	☐ **2** A **limited adverse effect** on an individual or agency	☒ **3** A **serious adverse effect** on an individual or agency	☐ **4** A **catastrophic effect** on an individual or agency

Category of Harm	Identity Assurance Impact Levels			
4. To what civil or criminal violations would the agency be subject (e.g., out of compliance with regulatory rules)?	☐ **1** **No** risk of civil or criminal violations	☐ **2** Risk of civil or criminal **violation**s that **would not** ordinarily be subject to enforcement efforts	☒ **3** Risk of civil or criminal **violation**s that **may be** subject to enforcement efforts	☐ **4** Risk of civil or criminal **violation**s that is of special importance to enforcement programs and may have **exceptionally grave consequences**
5. What harm to agency programs or public interest would be realized?	☐ **1** **No adverse effect** on any agency program, asset or the public interest	☐ **2** A **limited adverse effect** on any agency program, asset or the public interest	☒ **3** A **serious adverse effect** on any agency program, asset or the public interest	☐ **4** A **severe or catastrophic effect** on any agency program, asset or the public interest
6. How would personal safety be impacted?	☒ **1** **No** risk of injury	☐ **2** A risk of injury **not requiring medical attention**	☐ **3** A risk of non-serious injury **requiring medical attention**	☐ **4** A risk of **serious** injury or **death**

The system's identity assurance level will be based on the selections in the table above. The right-most checked impact level should be the overall identity assurance level assigned to the system.				
Identity Assurance Level Required	☐ **1** Low or no confidence in the asserted ***identity***'s validity	☐ **2** Confidence in the asserted ***identity's*** validity	☒ **3** High confidence in the asserted ***identity***'s validity	☐ **4** Very high confidence in the asserted ***identity***'s validity

Information Owner Date

EISO Representative Date