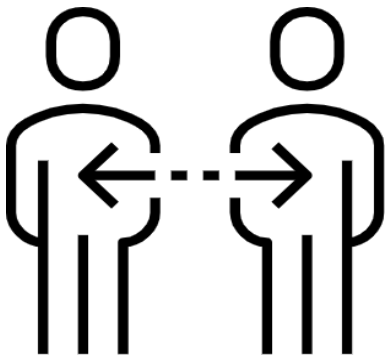


Learning Scenario: Deidentifying Personal Information – DEF/PMF

	<p>Program or Service: Deidentifying Personal Information</p> <p>GoA Staff: Data Analysts</p> <p>Lifecycle Stage: Data Use/Access, Storage/Management</p> <p>DEF Principles: Privacy and Protection, Transparency</p> <p>PMF Principles: Security and Control, Accountability, Openness</p>
<p>A ministry that provides services to Albertans has a dataset containing personal information about program clients that would be useful in determining future policy direction.</p> <p>Casey leads the team that is providing the analysis of the data and is responsible for determining whether the personal information is necessary for the analysis to be useful.</p> <p>In the analysis, Casey refers to the DEF principle of Privacy and Protection, which recommends analyzing the risks and benefits of deidentification for the purpose of re-using data, in addition to a legislative review with subject matter experts. Casey also refers to the PMF principle of Security and Control which highlights the need to proactively ensure the necessary safeguards, such as appropriate access restrictions, are in place to mitigate potential privacy risks (i.e., misuse of deidentified data that could result in reidentification).</p> <p>As part of this analysis, the program area also connected with the Privacy Services team to review the ability to leverage this dataset for this purpose and to discuss proposed steps for deidentification. Casey also engaged Cybersecurity Services to review existing safeguards of the program area’s system to ensure the necessary security controls are in place to manage the original and deidentified dataset.</p> <p>After careful consideration of how deidentifying the personal information in the dataset could affect the accuracy and meaningfulness of the data, Casey, through consultation with and recommendations from subject matter experts, concludes the dataset can be deidentified.</p> <p>Based on advice, Casey directs the team to remove personal information to create a new dataset. Additional direction was provided to the team that both the deidentified and original dataset are to remain in the program area’s system that has the appropriate user controls in place. By ensuring these processes are in place, Casey ensured the team followed the PMF principle of Accountability.</p> <p>Following the DEF principle of Transparency, the team documents the original source of the data, restrictions on the possible use of the data, and the processes used to derive the deidentified dataset from the original data. This also aligns with the PMF principle of Openness as the documentation allows the information pertaining to how the personal information is used to be readily available to Albertans.</p>	