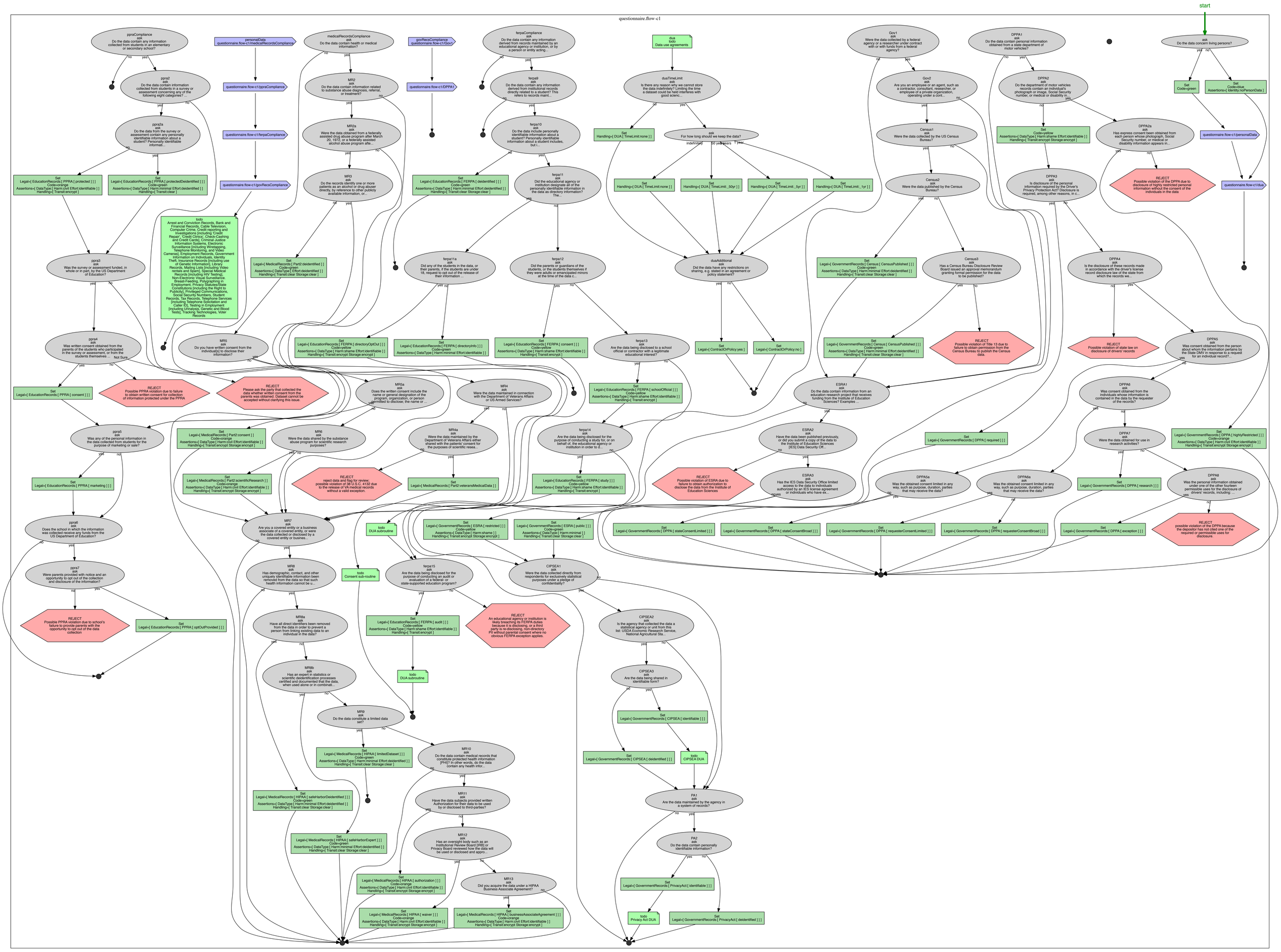
start
questionnaire.flow-c1
ask
Do the data concern living persons?
Set
Code=green
Set
Code=blue
Assertions=[Identity:noPersonData]
ppraCompliance
ask
Do the data contain any information collected from students in an elementary or secondary school?
ppra2
ask
Do the data contain information collected from students in a survey or assessment concerning any of the following eight categories?...
ppra2a
ask
Do the data from the survey or assessment contain any personally identifiable information about a student? Personally identifiable informati...
Set
Legal=[EducationRecords:[PPRA:[protected]]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt]
Set
Legal=[EducationRecords:[PPRA:[protectedDeidentified]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear]
ppra3
ask
Was the survey or assessment funded, in whole or in part, by the US Department of Education?
ppra4
ask
Was written consent obtained from the parents of the students who participated in the survey or assessment, or from the students themselves ...
Set
Legal=[EducationRecords:[PPRA:[consent]]]
REJECT
Possible PPRA violation due to failure to obtain written consent for collection of information protected under the PPRA
ppra5
ask
Was any of the personal information in the data collected from students for the purpose of marketing or sale?
Set
Legal=[EducationRecords:[PPRA:[marketing]]]
ppra6
ask
Does the school in which the information was collected receive any funds from the US Department of Education?
ppra7
ask
Were parents provided with notice and an opportunity to opt out of the collection and disclosure of the information?
REJECT
Possible PPRA violation due to school's failure to provide parents with the opportunity to opt out of the data collection
Set
Legal=[EducationRecords:[PPRA:[optOutProvided]]]
personalData
questionnaire.flow-c1/medicalRecordsCompliance
questionnaire.flow-c1/ppraCompliance
questionnaire.flow-c1/ferpaCompliance
questionnaire.flow-c1/govRecsCompliance
todo
Arrest and Conviction Records, Bank and Financial Records, Cable Television, Computer Crime, Credit reporting and Investigations [including 'Credit Repair', 'Credit Clinics', Check-Cashing and Credit Cards], Criminal Justice Information Systems, Electronic Surveillance [including Wiretapping, Telephone Monitoring, and Video Cameras], Employment Records, Government Information on Individuals, Identity Theft, Insurance Records [including use of Genetic Information], Library Records, Mailing Lists [including Video rentals and Spam], Special Medical Records [including HIV Testing], Non-Electronic Visual Surveillance, Breast-Feeding, Polygraphing in Employment, Privacy Statutes/State Constitutions [including the Right to Publicity], Privileged Communications, Social Security Numbers, Student Records, Tax Records, Telephone Services [including Telephone Solicitation and Caller ID], Testing in Employment [including Urinalysis, Genetic and Blood Tests], Tracking Technologies, Voter Records
medicalRecordsCompliance
ask
Do the data contain health or medical information?
MR2
ask
Do the data contain information related to substance abuse diagnosis, referral, or treatment?
MR2a
ask
Were the data obtained from a federally assisted drug abuse program after March 20, 1972, or a federally assisted alcohol abuse program afte...
MR3
ask
Do the records identify one or more patients as an alcohol or drug abuser directly, by reference to other publicly available information, or...
Set
Legal=[MedicalRecords:[Part2:deidentified]]
Code=green
Assertions=[DataType:[Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
MR5
ask
Do you have written consent from the individual(s) to disclose their information?
MR5a
ask
Does the written consent include the name or general designation of the program, organization, or person permitted to disclose; the name or ...
MR4
ask
Were the data maintained in connection with the Department of Veterans Affairs or US Armed Services?
MR4a
ask
Were the data maintained by the Department of Veterans Affairs either shared with the patients' consent for the purposes of scientific resea...
Set
Legal=[MedicalRecords:[Part2:veteransMedicalData]]
MR6
ask
Were the data shared by the substance abuse program for scientific research purposes?
Set
Legal=[MedicalRecords:[Part2:consent]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
Set
Legal=[MedicalRecords:[Part2:scientificResearch]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
REJECT
reject data and flag for review; possible violation of 38 U.S.C. 4132 due to the release of VA medical records without a valid exception.
MR7
ask
Are you a covered entity or a business associate of a covered entity, or were the data collected or disclosed by a covered entity or business...
MR8
ask
Has demographic, contact, and other uniquely identifiable information been removed from the data so that such health information cannot be u...
MR8a
ask
Have all direct identifiers been removed from the data in order to prevent a person from linking existing data to an individual in the data?
MR8b
ask
Has an expert in statistics or scientific deidentification processes certified and documented that the data, when used alone or in combinati...
MR9
ask
Do the data constitute a limited data set?
Set
Legal=[MedicalRecords:[HIPAA:[limitedDataset]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
MR10
ask
Do the data contain medical records that constitute protected health information [PHI]? In other words, do the data contain any health infor...
Set
Legal=[MedicalRecords:[HIPAA:[safeHarborDeidentified]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
MR11
ask
Have the data subjects provided written Authorization for their data to be used by or disclosed to third-parties?
Set
Legal=[MedicalRecords:[HIPAA:[safeHarborExpert]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
MR12
ask
Has an oversight body such as an Institutional Review Board [IRB] or Privacy Board reviewed how the data will be used or disclosed and appro...
Set
Legal=[MedicalRecords:[HIPAA:[authorization]]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
MR13
ask
Did you acquire the data under a HIPAA Business Associate Agreement?
Set
Legal=[MedicalRecords:[HIPAA:[waiver]]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
Set
Legal=[MedicalRecords:[HIPAA:[businessAssociateAgreement]]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
govRecsCompliance
questionnaire.flow-c1/DPPA1
ferpaCompliance
ask
Do the data contain any information derived from records maintained by an educational agency or institution, or by a person or entity acting...
ferpa9
ask
Do the data contain any information derived from institutional records directly related to a student? This refers to records maint...
ferpa10
ask
Do the data include personally identifiable information about a student? Personally identifiable information about a student includes, but i...
Set
Legal=[EducationRecords:[FERPA:[deidentified]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
ferpa11
ask
Did the educational agency or institution designate all of the personally identifiable information in the data as directory information? The...
ferpa11a
ask
Did any of the students in the data, or their parents, if the students are under 18, request to opt out of the release of their information ...
ferpa12
ask
Did the parents or guardians of the students, or the students themselves if they were adults or emancipated minors at the time of the data c...
Set
Legal=[EducationRecords:[FERPA:[directoryOptOut]]]
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
Set
Legal=[EducationRecords:[FERPA:[directoryInfo]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:identifiable]]
Set
Legal=[EducationRecords:[FERPA:[consent]]]
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt]
ferpa13
ask
Are the data being disclosed to a school official or contractor with a legitimate educational interest?
Set
Legal=[EducationRecords:[FERPA:[schoolOfficial]]]
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt]
ferpa14
ask
Are the data being disclosed for the purpose of conducting a study for, or on behalf of, the educational agency or institution in order to d...
Set
Legal=[EducationRecords:[FERPA:[study]]]
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt]
ferpa15
ask
Are the data being disclosed for the purpose of conducting an audit or evaluation of a federal- or state-supported education program?
Set
Legal=[EducationRecords:[FERPA:[audit]]]
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt]
REJECT
An educational agency or institution is likely breaching its FERPA duties because it is disclosing, or a third party is re-disclosing, non-directory PII without parental consent where no obvious FERPA exception applies.
todo
DUA subroutine
todo
Consent sub-routine
todo
DUA subroutine
dua
todo
Data use agreements
duaTimeLimit
ask
Is there any reason why we cannot store the data indefinitely? Limiting the time a dataset could be held interferes with good scienc...
Set
Handling=[DUA:[TimeLimit:none]]
ask
For how long should we keep the data?
indefinitely
50 years
5 years
1 year
Set
Handling=[DUA:[TimeLimit:none]]
Set
Handling=[DUA:[TimeLimit:_50yr]]
Set
Handling=[DUA:[TimeLimit:_5yr]]
Set
Handling=[DUA:[TimeLimit:_1yr]]
duaAdditional
ask
Did the data have any restrictions on sharing, e.g. stated in an agreement or policy statement?
Set
Legal=[ContractOrPolicy:yes]]
Set
Legal=[ContractOrPolicy:no]]
Set
Legal=[GovernmentRecords:[FERPA:[study]]]
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt]
Set
Legal=[GovernmentRecords:[ESRA:[restricted]]]
Code=yellow
Assertions=[DataType:[Harm:shame]]
Handling=[Transit:encrypt Storage:encrypt]
Set
Legal=[GovernmentRecords:[ESRA:[public]]]
Code=green
Assertions=[DataType:[Harm:minimal]]
Handling=[Transit:clear Storage:clear]
CIPSEA1
ask
Were the data collected directly from respondents for exclusively statistical purposes under a pledge of confidentiality?
CIPSEA2
ask
Is the agency that collected the data a statistical agency or unit from this list: USDA Economic Research Service, National Agricultural Sta...
CIPSEA3
ask
Are the data being shared in identifiable form?
Set
Legal=[GovernmentRecords:[CIPSEA:[identifiable]]]
Set
Legal=[GovernmentRecords:[CIPSEA:[deidentified]]]
todo
CIPSEA:DUA
PA1
ask
Are the data maintained by the agency in a system of records?
PA2
ask
Do the data contain personally identifiable information?
Set
Legal=[GovernmentRecords:[PrivacyAct:[identifiable]]]
todo
Privacy Act DUA
Set
Legal=[GovernmentRecords:[PrivacyAct:[deidentified]]]
Gov1
ask
Were the data collected by a federal agency or a researcher under contract with or with funds from a federal agency?
Gov2
ask
Are you an employee or an agent, such as a contractor, consultant, researcher, or employee of a private organization, operating under a cont...
Census1
ask
Were the data collected by the US Census Bureau?
Census2
ask
Were the data published by the Census Bureau?
Census3
ask
Has a Census Bureau Disclosure Review Board issued an approval memorandum granting formal permission for the data to be published?
Set
Legal=[GovernmentRecords:[Census:[CensusPublished]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
Set
Legal=[GovernmentRecords:[Census:[CensusPublished]]]
Code=green
Assertions=[DataType:[Harm:minimal Effort:deidentified]]
Handling=[Transit:clear Storage:clear]
REJECT
Possible violation of Title 13 due to failure to obtain permission from the Census Bureau to publish the Census data.
ESRA1
ask
Do the data contain information from an education research project that receives funding from the Institute of Education Sciences? Examples ...
ESRA2
ask
Have the data been published previously, or did you submit a copy of the data to the Institute of Education Sciences (IES) Data Security Off...
ESRA3
ask
Has the IES Data Security Office limited access to the data to individuals authorized by an IES license agreement or individuals who have ex...
REJECT
Possible violation of ESRA due to failure to obtain authorization to disclose the data from the Institute of Education Sciences
Set
Legal=[GovernmentRecords:[DPPA:[required]]]
DPPA1
ask
Do the data contain personal information obtained from a state department of motor vehicles?
DPPA2
ask
Do the department of motor vehicles records contain an individual's photograph or image, Social Security number, or medical or disability in...
Set
Code=yellow
Assertions=[DataType:[Harm:shame Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
DPPA2a
ask
Has express consent been obtained from each person whose photograph, Social Security number, or medical or disability information appears in...
questionnaire.flow-c1/personalData
DPPA3
ask
Is disclosure of the personal information required by the Driver's Privacy Protection Act? Disclosure is required, among other reasons, in c...
REJECT
Possible violation of the DPPA due to disclosure of highly restricted personal information without the consent of the individuals in the data
questionnaire.flow-c1/dua
DPPA4
ask
Is the disclosure of these records made in accordance with the driver's license record disclosure law of the state from which the records we...
REJECT
Possible violation of state law on disclosure of drivers' records
DPPA5
ask
Was consent obtained from the person about whom the information pertains by the State DMV in response to a request for an individual record?...
DPPA6
ask
Was consent obtained from the individuals whose information is contained in the data by the requester of the records?
DPPA7
ask
Were the data obtained for use in research activities?
Set
Legal=[GovernmentRecords:[DPPA:[highlyRestricted]]]
Code=orange
Assertions=[DataType:[Harm:civil Effort:identifiable]]
Handling=[Transit:encrypt Storage:encrypt]
Set
Legal=[GovernmentRecords:[DPPA:[research]]]
DPPA8
ask
Was the personal information obtained under one of the other fourteen permissible uses for the disclosure of drivers' records, including: ...
REJECT
possible violation of the DPPA because the depositor has not cited one of the required or permissible uses for disclosure.
DPPA5a
ask
Was the obtained consent limited in any way, such as purpose, duration, parties that may receive the data?
DPPA6a
ask
Was the obtained consent limited in any way, such as purpose, duration, parties that may receive the data?
Set
Legal=[GovernmentRecords:[DPPA:[stateConsentLimited]]]
Set
Legal=[GovernmentRecords:[DPPA:[stateConsentBroad]]]
Set
Legal=[GovernmentRecords:[DPPA:[requesterConsentLimited]]]
Set
Legal=[GovernmentRecords:[DPPA:[requesterConsentBroad]]]
Set
Legal=[GovernmentRecords:[DPPA:[exception]]]