start
DecisionGraph-1
questionnaire.dg/global-start ask Do the data concern living persons?
Set DataTags: Code=green
Set DataTags: Code=blue Assertions: Identity=noPersonData
questionnaire.dg/filter-medical ask Do the data contain health or medical information?
medical.dg/ medicalSection
questionnaire.dg/filter-ppra ask Was the data collected from students in an elementary or secondary school?
ppra.dg/ ppraSection
questionnaire.dg/filter-ferpa ask Do the data contain any information derived from ministry of education data?
ferpa.dg/ ferpaSection
government-records.dg/ govSection
dppa.dg/ dppaSection
questionnaire.dg/futures todo Future additions go here.
questionnaire.dg/ pDUA
Part [ferpa.dg]ferpaSection
Family Education Records Protection Act
ferpa.dg/start ask Do the data contain any information derived from institutional records directly related to a student?
ferpa.dg/ferpa10 ask Do the data include personally identifiable information about a student?
Set DataTags: Legal: EducationRecords: FERPA+=deidentified Code=green Assertions: DataType: Harm=minimal Effort=deidentified Handling: Storage=clear Transit=clear
ferpa.dg/ferpa11 ask Did the educational agency or institution designate all of the personally identifiable information in the data as directory information?
ferpa.dg/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 ...
ferpa.dg/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 DataTags: Legal: EducationRecords: FERPA+=directoryOptOut Code=yellow Assertions: DataType: Harm=shame Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt
Set DataTags: Legal: EducationRecords: FERPA+=directoryInfo Code=green Assertions: DataType: Harm=minimal Effort=identifiable
Set DataTags: Legal: EducationRecords: FERPA+=consent Code=yellow Assertions: DataType: Harm=shame Effort=identifiable Handling: Transit=encrypt
todo Consent sub-routine
ferpa.dg/ferpa13 ask Are the data being disclosed to a school official or contractor with a legitimate educational interest?
Set DataTags: Legal: EducationRecords: FERPA+=schoolOfficial Code=yellow Assertions: DataType: Harm=shame Effort=identifiable Handling: Transit=encrypt
ferpa.dg/ferpa14 ask Are the data being disclosed for a purpose allowed by law?
Set DataTags: Legal: EducationRecords: FERPA+=study Code=yellow Assertions: DataType: Harm=shame Effort=identifiable Handling: Transit=encrypt
ferpa.dg/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 DataTags: Legal: EducationRecords: FERPA+=audit Code=yellow Assertions: DataType: Harm=shame Effort=identifiable Handling: Transit=encrypt
REJECT FERPA violation by disclosing data that should not be disclosed.
todo DUA subroutine
Part [dppa.dg]dppaSection
Driver's Privacy Protection Act
dppa.dg/DPPA1 ask Do the data contain personal information obtained from a state department of motor vehicles?
dppa.dg/DPPA2 ask Do the DMV records contain PII?
dppa.dg/DPPA2a ask Did you get conscent from the data subjects?
Set DataTags: Code=yellow Assertions: DataType: Harm=shame Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt
Set DataTags: Legal: GovernmentRecords: DPPA+=highlyRestricted Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt
REJECT DPPA violation
dppa.dg/DPPA3 ask Is disclosure of the personal information required by the Driver's Privacy Protection Act?
Set DataTags: Legal: GovernmentRecords: DPPA+=required
dppa.dg/DPPA4 ask Is the disclosure of these records made in accordance with the driver's license record disclosure law (state law)?
REJECT Possible violation of state law on disclosure of drivers' records
dppa.dg/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?
dppa.dg/DPPA5a ask Was the obtained consent limited in any way, such as purpose, duration, parties that may receive the data?
dppa.dg/DPPA6 ask Was consent obtained from the individuals whose information is contained in the data by the requester of the records?
Set DataTags: Legal: GovernmentRecords: DPPA+=stateConsentLimited
Set DataTags: Legal: GovernmentRecords: DPPA+=stateConsentBroad
dppa.dg/DPPA6a ask Was the obtained consent limited in any way, such as purpose, duration, parties that may receive the data?
dppa.dg/DPPA7 ask Were the data obtained for use in research activities?
Set DataTags: Legal: GovernmentRecords: DPPA+=requesterConsentLimited
Set DataTags: Legal: GovernmentRecords: DPPA+=requesterConsentBroad
Set DataTags: Legal: GovernmentRecords: DPPA+=research
dppa.dg/DPPA8 ask Was the personal information obtained under one of the other fourteen permissible uses for the disclosure of drivers' records?
Set DataTags: Legal: GovernmentRecords: DPPA+=exception
REJECT possible violation of the DPPA: depositor has not cited one of the required or permissible uses for disclosure.
Part [government-records.dg]govSection
Government Records
government-records.dg/Gov1 ask Were the data collected by a federal agency or a researcher under contract with or with funds from a federal agency?
government-records.dg/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...
government-records.dg/Census1 ask Were the data collected by the US Census Bureau?
government-records.dg/Census2 ask Were the data published by the Census Bureau?
Set DataTags: Assertions: DataType: Harm=minimal Effort=deidentified Code=green Handling: Transit=clear Storage=clear Legal: GovernmentRecords: Census+=CensusPublished
government-records.dg/Census3 ask Has a Census Bureau Disclosure Review Board issued an approval memorandum granting formal permission for the data to be published?
Set DataTags: Assertions: DataType: Harm=minimal Effort=deidentified Code=green Handling: Transit=clear Storage=clear Legal: GovernmentRecords: Census+=CensusPublished
REJECT Possible violation of Title 13 due to failure to obtain permission from the Census Bureau to publish the Census data.
government-records.dg/ESRA1 ask Do the data contain information from an education research project that receives funding from the Institute of Education Sciences? Examples ...
government-records.dg/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...
government-records.dg/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 DataTags: Code=yellow Assertions: DataType: Harm=shame Handling: Transit=encrypt Storage=serverEncrypt Legal: GovernmentRecords: ESRA+=restricted
Set DataTags: Code=green Assertions: DataType: Harm=minimal Handling: Transit=clear Storage=clear Legal: GovernmentRecords: ESRA+=public
government-records.dg/CIPSEA1 ask Were the data collected directly from respondents for exclusively statistical purposes under a pledge of confidentiality?
government-records.dg/CIPSEA2 ask Is the agency that collected the data a statistical agency or unit from this list: USDA Economic Research Service, National Agricultural Sta...
government-records.dg/CIPSEA3 ask Are the data being shared in identifiable form?
Set DataTags: Legal: GovernmentRecords: CIPSEA+=identifiable
todo CIPSEA DUA
Set DataTags: Legal: GovernmentRecords: CIPSEA+=deidentified
government-records.dg/PA1 ask Are the data maintained by the agency in a system of records?
government-records.dg/PA2 ask Do the data contain personally identifiable information?
Set DataTags: Legal: GovernmentRecords: PrivacyAct+=identifiable
Set DataTags: Legal: GovernmentRecords: PrivacyAct+=deidentified
todo Privacy Act DUA
Part [ppra.dg]ppraSection
Protection of Pupil Rights Amendment
ppra.dg/start ask Do the data contain information collected from students in a survey or assessment concerning any of the covered categories?
ppra.dg/ppra2a ask Do the data contain any student PII?
Set DataTags: Legal: EducationRecords: PPRA+=protected Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt
Set DataTags: Legal: EducationRecords: PPRA+=protectedDeidentified Code=green Assertions: DataType: Harm=minimal Effort=deidentified Handling: Transit=clear Storage=clear
ppra.dg/ppra3 ask Was the survey or assessment funded, in whole or in part, by the US Department of Education?
ppra.dg/ppra4 ask Was written consent obtained from the parents or students prior to the data collection?
Not Sure
ppra.dg/ppra5 ask Was any of the personal information in the data collected from students for the purpose of marketing or sale?
Set DataTags: Legal: EducationRecords: PPRA+=consent
REJECT Possible PPRA violation - no collection consent
REJECT Please clarify wheather a consent was obtained.
Set DataTags: Legal: EducationRecords: PPRA+=marketing
ppra.dg/ppra6 ask Does the school in which the information was collected receive any funds from the US Department of Education?
ppra.dg/ppra7 ask Were parents provided with notice and an opportunity to opt out of the collection and disclosure of the information?
Set DataTags: Legal: EducationRecords: PPRA+=optOutProvided
REJECT Possible PPRA violation due to school's failure to provide parents with the opportunity to opt out of the data collection
Part [questionnaire.dg]pDUA
Section Data Use Agreements
Data Use Agreements
questionnaire.dg/dua-ext todo Data use agreements
questionnaire.dg/duaTimeLimit ask Is there any reason why we cannot store the data indefinitely?
ask For how long should we keep the data?
indefinitely 5 years 50 years 2 years 1 year
Set DataTags: Handling: DUA: TimeLimit=none
Set DataTags: Handling: DUA: TimeLimit=none
Set DataTags: Handling: DUA: TimeLimit=_50yr
Set DataTags: Handling: DUA: TimeLimit=_5yr
Set DataTags: Handling: DUA: TimeLimit=_2yr
Set DataTags: Handling: DUA: TimeLimit=_1yr
questionnaire.dg/duaAdditional ask Did the data have any restrictions on sharing, e.g. stated in an agreement or policy statement?
Set DataTags: Legal: ContractOrPolicy=yes
Set DataTags: Legal: ContractOrPolicy=no
Part [medical.dg]medicalSection
Medical Records
medical.dg/start ask Do the data contain information related to substance abuse diagnosis, referral, or treatment?
medical.dg/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...
medical.dg/MR3 ask Do any of the substance abuse records contain direct or referential PII?
medical.dg/MR4 ask Were the data maintained in connection with the US Department of Veterans Affairs or US Armed Services?
medical.dg/MR4a ask Were the data maintained by the Department of Veterans Affairs either shared with the patients' consent for the purposes of scientific resea...
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.
Set DataTags: Legal: MedicalRecords: Part2=veteransMedicalData Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Transit=encrypt
medical.dg/MR5 ask Did the individuals provide written consent for the disclosure of their information?
Set DataTags: Legal: MedicalRecords: Part2=consent Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt
medical.dg/MR6 ask Were the data shared by the substance abuse program for scientific research purposes?
Set DataTags: Legal: MedicalRecords: Part2=scientificResearch Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt
Set DataTags: Legal: MedicalRecords: Part2=deidentified Assertions: DataType: Effort=deidentified Handling: Storage=clear Transit=clear Code=green
medical.dg/MR7 ask Do the data contain information from a covered entity or business associate of a covered entity?
Not Sure
REJECT The PII issue has to be cleared before depositing the data.
medical.dg/MR8 ask Have all direct identifiers been removed from the data?
Set DataTags: Legal: MedicalRecords: HIPAA+=safeHarborDeidentified Code=green Assertions: DataType: Harm=minimal Effort=deidentified Handling: Transit=clear Storage=clear
medical.dg/MR8a ask Has an expert in statistical or scientific principles and methods for deidentification certified that the data have been deidentified?
Set DataTags: Legal: MedicalRecords: HIPAA+=expertDetermination Code=green Assertions: DataType: Harm=minimal Effort=deidentified Handling: Transit=clear Storage=clear
medical.dg/MR9 ask Do the data constitute a limited data set under the HIPAA Privacy Rule?
Set DataTags: Legal: MedicalRecords: HIPAA+=limitedDataset Code=green Assertions: DataType: Harm=minimal Effort=deidentified Handling: Transit=clear Storage=clear
medical.dg/MR10 ask Do the data contain protected health information from medical records?
medical.dg/MR11 ask Do the data contain health information from patients who have provided written authorization for their information to be disclosed to or use...
Set DataTags: Legal: MedicalRecords: HIPAA+=authorization Assertions: DataType: Harm=civil Effort=identifiable Code=orange Handling: Transit=encrypt Storage=serverEncrypt
medical.dg/MR12 ask Has an oversight body reviewed how the data will be used or disclosed and approved a request to alter or waive the Authorization requirement...
Set DataTags: Legal: MedicalRecords: HIPAA+=waiver Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Storage=serverEncrypt Transit=encrypt
medical.dg/MR13 ask Were the data disclosed pursuant to a HIPAA business associate contract?
Set DataTags: Legal: MedicalRecords: HIPAA+=businessAssociateContract Code=orange Assertions: DataType: Harm=civil Effort=identifiable Handling: Transit=encrypt Storage=serverEncrypt