How to Translate Legalese for Technologists

Baron Rodriguez
Executive Director
Data Integration Support Center

Marion McWilliams
Staff Lead Attorney
Data Integration Support Center

Welcome!

Add to the chat:

- Name, organization, sector
- On a scale of 1-10, how much is data, or questions about data, part of your regular work?
- What summer activity are you looking forward to that you haven't done yet?

What we do

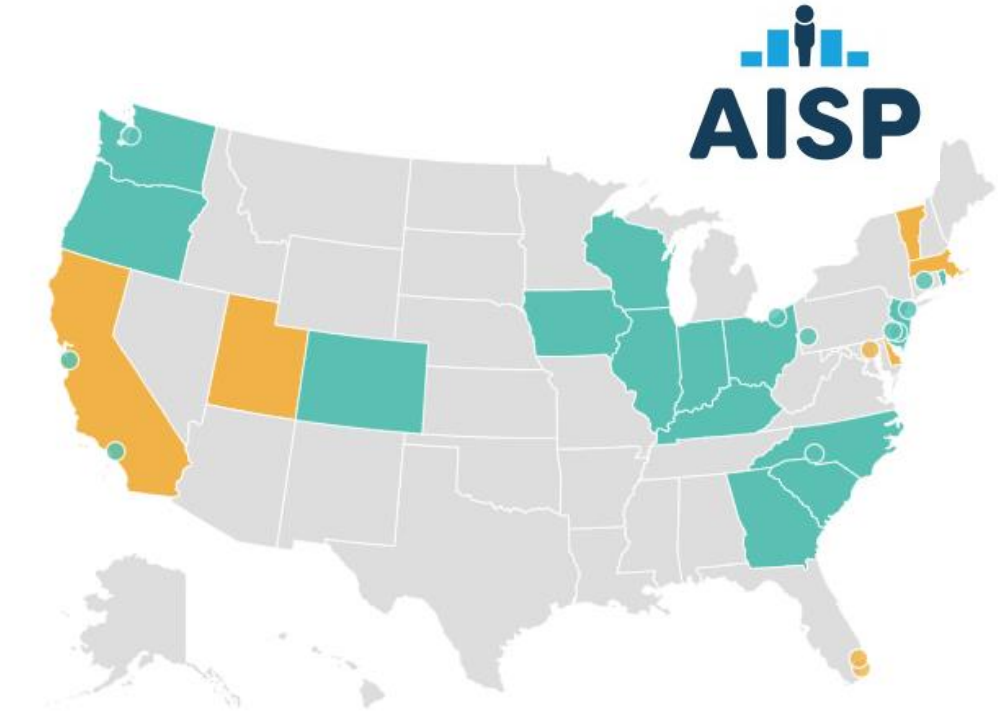
AISP

- IDS Peer Network
- Guidance & Standards
- Training & Consulting
- Advocacy & Communications
- Multi-site Research

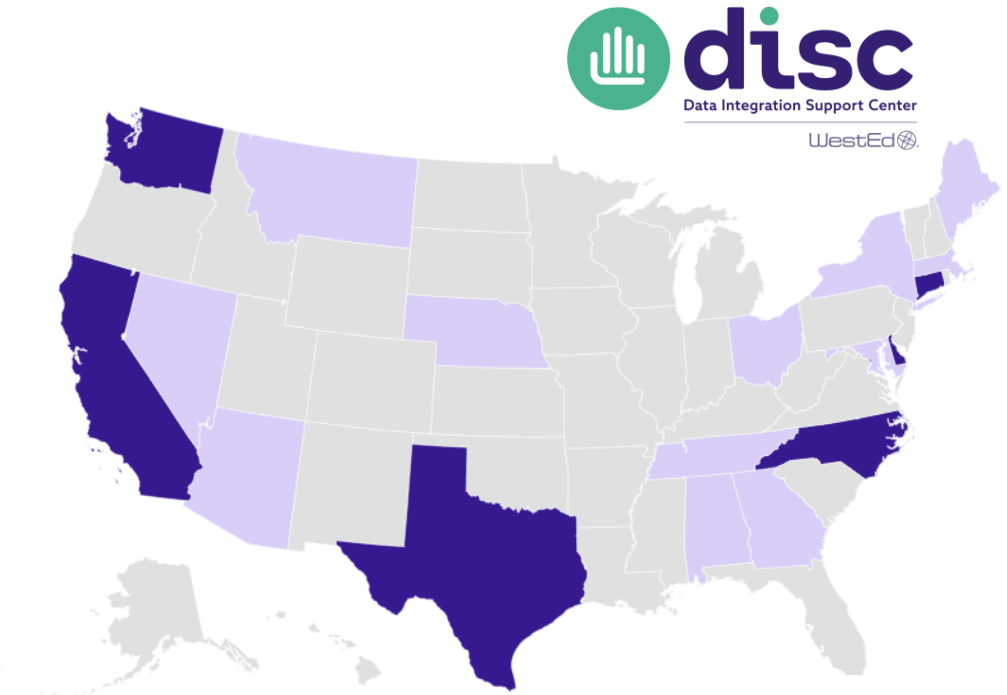
DISC

- Planning & User-Centered Design
- Legislative Analysis
- External Legal Support
- Privacy
- System Security

Our Networks



Network Sites Developing Sites



Intensive TA support Moderate TA support

ESSENTIAL QUESTIONS

What are the key challenges faced by technologists when working with lawyers and how can these challenges be overcome?

What are the essential legal concepts that technologists need to understand in their cross-functional collaboration with legal departments?

In what ways can technologists contribute meaningfully to discussions about legal advice and counsel, considering their understanding of legal concepts and language?

Foundational Concepts

Relationships Matter

Trust is critical to developing common language, eliminating "lane changes", and building respect of each professional's role.

Understand Perspective

Attorneys focus on identification and reduction of risk to the organization. It is a critical role in data integration efforts. They have no interest in making your job more difficult.

Practice Makes Perfect

Following the first two concepts will naturally allow for "rhythm" to develop between the technology teams and their legal teams in the development of new legal documents or understanding responsibilities in the event of an incident.

Moonlighting Roles

Building computers at home does not make you a technology expert.

JUST LIKE…

Watching Judge Judy doesn't make you an attorney.

Key Terms

For each of the terms, we will share a common legal definition, use case, and common miscommunication and/or misunderstandings via properly deidentified scenarios.

- **Data Breach**
- **MOU**
- **DSA/DUA**
- **Disclosure**
- **Deidentification**
- **Security Incident**
- **Data Destruction**

Understanding roles, responsibilities, procedures, and establishing training for your organization is key to ensuring Technology and Legal teams are on the same page!

Terminology, Definitions, & Scenarios

Oh my!!

Data Breach

Definition*

A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual. It could be a result of:

- hacking
- theft of credit/debit card numbers
- lost, discarded or stolen documents/devices
- mishandled sensitive information

Common Issues

- There is a stark difference between a security incident, a data breach, and a reportable data breach. Cooperation between Legal & Technology is ESSENTIAL to determining the extent and response.
- Notification responsibilities vary WIDELY based on type of data, impacted individuals, location of subjects impacted by the breach, and any legal agreements implicated by the breach.

Scenario

- Staff member sends notification to attorney, self admitting a "data breach"
- Attorney works on preparing a response/letter to the organization
- Incident response plan, completely housed in IT, was not utilized
- Security/Data incident procedure was not read, or followed by the employee who went straight to Legal

* Source: PrivacyRights.org

Memorandums of Understanding/Agreement

Definition*	Common Issues	Scenario
[Usually] a non-binding agreement, letter or similar document that sets forth two or more parties' intent to collaborate or pursue some future activity. A MOU may provide a description of the proposed collaboration or future activity, except as may be set forth in a subsequent legally-binding agreement.	• Technologists often utilize that term loosely and with the wrong audience, it may not be well understood that you are seeking a binding agreement. • Some attorneys will build legally binding MOUs that set the basic terms of engagement, such as indemnification, breach response, statutory/regulatory references and other static terms that can be agreed to as a start for IDS participation.	• "You got what you asked for!"

* Source: Harvard T.H. Chan School of Public Health Research Administration: Agreement Types

Data Use Agreement/Data Sharing Agreement

Definition*	Common Issues	Scenario
A Data Use Agreement (DUA) is a binding contract between organizations governing the transfer and use of data. The transfer of data between organizations is common in the research community. When the data is confidential, proprietary, or otherwise considered sensitive, the organization providing the data ("Provider") will often require that the organization receiving the data ("Recipient") enter into a written contract to outline the terms and conditions of the data transfer.	• Needlessly tweaking static terms for each engagement with every DUA/DSA • Inconsistency of security, privacy, or data requirements because terms aren't regularly updated as technology systems change or access controls change	• FERPA 2011 Regulatory Changes

* Source: Harvard T.H. Chan School of Public Health Research Administration: Agreement Types

Disclosure

Definition*	Common Issues	Scenario
Disclosure means to permit access to, or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.	• Restricting access to properly deidentified data or summary data under the premise of an unauthorized redisclosure • Misunderstanding around authorized versus unauthorized disclosures	• Tech & attorney talking over each other

* Source: U.S. Department of Ed Student Privacy Policy Office

Deidentification

Definition*

Refers to the process of removing or obscuring any personally identifiable information from student records in a way that minimizes the risk of unintended disclosure of the individuals and information about them. (Reasonable person)

Privacy Term: Anonymization: refers to the process of data de-identification which produces de-identified data, where individual records cannot be linked back to an original student record system or to other individual records from the same source, because they do not include a record code needed to link the records.

Common Issues

- Use case is critical. There are reasons for general deidentification versus true anonymization
- Deidentification may not be sufficient for public data sets as there may be complimentary suppression considerations if other data is also available

Scenario

- Not everyone is a privacy, statistical, or legal professional

* Source: U.S. Department of Ed Student Privacy Policy Office

Security Incident

Definition*	Common Issues	Scenario
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	• A data breach is a security incident, but a security incident is not necessarily a data breach • Overreacting can cause more harm than good until the true nature of the incident is understood	• The case of “missing data”

* Source: NIST

Alternative Solutions

Privacy Officers

DISC

Practical Solutions

- Build glossaries
- Document processes, roles and responsibilities, and points of contact
- Practice doomsday scenarios
- Train, train, train!

Questions?

Closing Reflections

TELL US IN THE CHAT:

What is one thing you are taking away from this training today?

Thank you.

For more trainings like this, check out: https://disc.wested.org/disc-aisp-legal-professionals-workshops/

Baron Rodriguez

Executive Director
Data Integration Support Center

info@DISC.WestEd.org

Marion McWilliams

Staff Lead Attorney
Data Integration Support Center

info@DISC.WestEd.org

A Project of WestEd