SIF® Association

Data Privacy, Security and Interoperability

…Making sure YOU are in charge of YOUR data

- ✓ **Data Interoperability** – *the sharing of data*
- ✓ **Data Security** – *the sharing of data in the right way*
- ✓ **Data Privacy** – *the sharing of data with the right person in the right way*

A little information can be a dangerous thing – and a lot of information possibly more!

Many times SIF presentations begin with three questions: How many in attendance have ever bought anything online? How many do all their banking online? How many know what their child got on a science test they took last week? The breakdown traditionally was always 2/3 to 1/3 to a very few, but that trend is changing.

People know they can get all kinds of real-time information online and now they expect to be able to get it from their children's school. The down side of this is that others want that information as well…

- *Data Breaches Surge in 2014 with 200 Million Data Records Stolen in First Three Months of the Year* (SafeNet, Inc.)
- *Prominent Ed-Tech Players' Data-Privacy Policies Attract Scrutiny* (Education Week)
- *State Lawmakers Ramp Up Attention to Data Privacy* (Education Week)

Headlines like these are being seen daily in the news - both inside and outside of education. The privacy issue is THE "hot button" topic for data management at all levels in the education enterprise. Numerous policy guidance documents have been drafted, legislation crafted, conferences held, effective practice shared and yet there seems to be a deft of actionable guidance and support provided "where the rubber hits the road" – the local schools where the data originates.

The Players	The Data Involved	The Questions
Parents of Students School / Local Authorities State Authority Federal Government Vendor whose product stores data and those who use the data Policy-maker The Learner	Student Identification Student Aggregations Student Academics Student Discipline Student Health Student Assessment Staffing Information	Who "has" the data? Who can access the data? Who determines access? Who is notified before data is accessed? Can they object? Who gets notified before the data is used in a new way? Who can change data? Who defines "ownership" rules and who enforces them?

In reality the larger question should be first addressed "***Why are we collecting these data points and who's core mission are they supporting?***" Is the answer - the Teacher? The Administrator? The Policy-maker? The Parent? The Learner?

Oftentimes the policies suggested by government, non-profit and even vendor entities are high level and do not address the realities of limited dollars, expertise and singular focus that schools survive within. Policies must make it crystal clear which players "own" which data since we also know data management is not a "solo shop" proposition. Schools, regional agencies and even states need to partner with marketplace providers to effectively manage and safeguard the data critical to their core missions. There needs to be commonly used privacy effective practices and technology strategies utilized by all players whether we are talking about spread sheets or total cloud-based enterprise models. As with most critical issues, the key is to communicate clear and unwavering expectations and work as a community to make them "on the ground realities".

The most effective and secure technical solutions need to be "hybrid" in nature. They must *transparently incorporate applications* deployed in the IT center and / or in the Cloud. They are *based upon "opt in" sharing* from one or more data sources (the *Data Confederacy* model[1]) rather than a required centralized data store not under the full control of the locale Educational Authority (the *Data Union* model).

The SIF Association is a community of schools, regional agencies, departments of education and marketplace working together to create safe student experiences. Solutions conforming to the SIF standard are based on a Data Confederacy model rather than a Data Union model. This allows local data privacy policies to be reflected in all SIF solutions, because all data sharing is an "opt in". The SIF technical blueprints define internal and external end point interfaces for marketplace products – the exact application boundaries where student data is shared - realizing that multi-application software solutions involve:

- ✓ **Data Interoperability** – the sharing of data
- ✓ **Data Security** – the sharing of data in the right way
- ✓ **Data Privacy** – the sharing of data with the right person in the right way

The SIF Standard was originally designed almost two decades ago to enable the first, has evolved to ensure the second, and now we are working to enforce the third! LEA and SEA site administrators using SIF enabled software strategies can control exactly what data is being shared between applications / users at a particular site without changing the application code - the critical piece of functionality needed to enforce Data Privacy policies for both on-site and cloud based Service.

The 3,200 members of the community have embarked on the mission to develop actionable privacy deliverables. A new ***SIF Data Privacy Work Group*** is concentrating on end user (District and State) issues relating to ensuring data privacy primarily for student data, but encompassing staff and possibly parental data privacy as well (Appendix A: Deliverables). SIF is a uniquely qualified player to take on the issue of data privacy, because it is a community of end users and vendors, working together to standardize application-to-application interoperability. Only when both groups are involved in the dialogue (and each is sharing their concerns) are viable solutions likely to result.

In the coming weeks you will be seeing more detailed information from this group – but why not get involved now and be a part of the deliverables and get your needs addressed? We would be happy to chat with you to see how the community can better support your needs, link you with other peers with the same issues and just find out how leveraging openly developed technical standards can benefit your work.

It is time, much like the parent getting the science grade on their child from last week, to get MORE information, this time on data privacy!

[1] *More information on Data Confederacy vs Data Union models can be found in the Centralized vs Distributed Education Architecture Solutions white paper on the SIF Association website: https://www.sifassociation.org/NewsRoom/White%20Papers/Centralized%20vs%20Distributed%20Educational%20Solution%20Architectures.pdf*

Appendix A: Deliverables

Checklist of Data Privacy "Recommendations": These suggest important SEA / LEA constraints be placed upon the privacy policies of Cloud Service providers, enabling EAs to meet or exceed FERPA and local data privacy mandates. Where such guidelines are not agreed to before sensitive student data is turned over to a Cloud Service vendor, data privacy can be fatally compromised with no recourse from the District or State.

Problematic vendor Data Privacy Clauses have and will continue to be identified, documented and used as the basis of constructing this checklist, which is anticipated to provide the basis for data privacy requirements in a district or state RFP.

Data Privacy Use Cases: These identify the major solution components (ex: District SIS, State Data Warehouse) and what sort of (student) data they each should be allowed access to in a particular process (and whether for all students or a subset).

> *Example A: Work Study Application (UK use case –only students in the work study program and only their identification and grades)*
>
> *Example B: State level Data Warehouse (Student Data without identification elements like name, addresses, phone numbers)*

Object Data Privacy "Profiles": Each profile will correspond to one or more use cases, and will identify a unique collection of (in the US CEDS-conformant) data elements which are to contained in objects conforming to that profile. For example the *Anonymous Student* profile might contain an encoded unique index (UUID) but no identifying student data elements (name, addresses, phone numbers, etc.). Other standardized profiles might exclude discipline or health related student elements or any combination of all 3.

Administrative Data Privacy "Best Practices": These will specify exactly how SIF-compliant solutions can be administrated to enforce selected Object Data Privacy Profiles in a real world solution. For example, once the *Anonymous Student* profile is selected, the multi-zone SIF Data Confederacy architecture allows local administrators to directly apply that profile to all student data exchanges in a separate *Anonymous Student* SIF Zone. The set of applications assigned to that Zone (whether cloud based or not) never see the restricted information … not because it is stripped out by routing middleware or just before message delivery, but because it is never made available to them.