Legal Subcommittee Meeting Summary

June 29, 2021

This document provides a summary of key points that emerged over the course of the meeting. More information about the meeting, including the PowerPoint and a meeting recording are available at https://cadatasystem.wested.org/meeting-information/legal-subcommittee.

The June 29, 2021 meeting had the following goals:

- Provide updates on the planning process
- Finalize the following items:
    - Master Data Exchange Agreement/Business Use Case Proposal
    - Participation Agreement

The following representatives attended the meeting:

Veronica Villalobos Cruz and Thomas Vu, Association for Independent California Colleges and Universities; Kathy Lynch, California Community College Chancellor's Office; Bruce Yonehiro of CDE, California Department of Education; Mike Arakji, California Department of General Services; Kary Marshall, California Department of Technology; Margaret Porto, California Department of Health Care Services; Carolyn Kubish, California Department of Social Services; Jennifer Schwartz, California Health and Human Services Agency; Rima Mendez, California School Information Services; Ed Hudson, Monique Shay, and John Walsh, California State University; Mark Paxson, California Student Aid Commission; Jeanne Wolfe, Labor and Workforce Development Agency; and Stella Ngai, University of California, Office of the President.

Master Data Exchange Agreement (MDEA)

After Kathy Booth of WestEd provided a synopsis of decisions from the June workgroup meeting, the subcommittee began reviewing edits to the MDEA.

Stella Ngai of UC indicated that her agency had not finished reviewing the document and had additional changes that had not yet been shared.

Purpose and Intent

Bruce Yonehiro of CDE noted that there is language on "incorporation by reference" twice and suggested consolidating the wording. He also asked for clarification on whether the terms of MDEA are part of the Business Use Case Proposal (BUCP) or vice versa. He suggested language changes that clarify MDEA is part of BUCP, which the subcommittee agreed to.

Special Compliance Provisions

Jennifer Schwartz of CHHS noted that language about the Business Associate Agreement (BAA) is specific to DHCS, which would need to be amended if other covered entities sign on in the future. In addition, HIPAA is routinely updated, so in the Modification section, language should be added that indicates Addendum A can be modified to address changes to federal law or additions of new data providers. Also, she noted that in her experience BUCPs often need to be updated when specific data elements are added or removed, which the signatories might want to document without having to re-execute the agreement. She suggested specific language changes, which the subcommittee agreed to.

Definitions

Marion McWilliams of WestEd raised a question about the definition of "data." If the "data" definition includes aggregated data, it could create a scenario where a plaintiff would have greater access to data than the data providers or the managing entity. This could be addressed by using the term "confidential data," as defined by the civil code. Bruce Yonehiro of CDE agreed.

Jennifer Schwartz of CHHS asked that the definition of "data" include language on modification or derivation. She also noted that aggregated data is not necessarily deidentified, so there will need to be data suppression in addition to aggregation.

Mike Arakji of the Department of General Services (DGS), who will serve as the information security officer for the Office of Cradle-to-Career, suggested that the document use the same definition for "data" that is laid out in the State Administrative Manual (SAM). State entities are required to adopt these definitions in their policies. He also provided the SAM definition for the term "confidential."

Stella Ngai of UC agreed that the SAM language should be used to define "confidential." This will be helpful if there are disputes about the nature of this term.

The subcommittee agreed to replace the word "data" with the term "confidential data" and to adjust the definition of "confidential" to align with SAM.

Jennifer Schwartz of CHHS cautioned that there are instances in the document where "data" is a generally defined term, so the WestEd team should be cautious about what gets replaced.

Bruce Yonehiro of CDE asked why language was removed that further clarifies that data "includes without limitation personally identifiable information."

Mike Arakji of DGS argued that the agreement should use the definition that has been adopted by the state. These are required by the Office of Information Security and the California Department of Technology in policies pertaining to audits of data systems.

Bruce Yonehiro of CDE noted that the extra phrase would be used in addition to the state definition to provide greater clarification.

The subcommittee agreed expand upon the SAM definition with the clarifying clause.

Mike Arakji of DGS asked why the suggested language for "data" includes both the terms "modification" and "alternation," which does not fit with terms used in data security practice. He outlined several terms that address the various states that data may be in.

Ed Hudson of CSU noted that while Mike Arakji of DGS is correct, using technical language may overly complicate the document.

Jennifer Schwartz of CHHS clarified that it will be important to use terms found in common non-technical circumstances. Bruce Yonehiro of CDE and Stella Ngai of UC agreed. Jennifer Schwartz of CHHS further noted that using both terms would allow for modification of data when it gets combined.

A member of the public asked whether the term "information" should also be defined.

Mike Arakji of DGS replied that there is no formal definition of “information” in the SAM, although the term “confidential information” is defined. However, the words “information” and “data” get used interchangeably in practice.

The subcommittee agreed to use the edited definition.

Marion McWilliams of WestEd noted suggested edits to the definition for “provider” to align with trailer bill statue and in other agreements.

The subcommittee agreed to use the edited definition.

Marion McWilliams of WestEd described changes suggested by Stella Ngai of UC pertaining to “destroy.”

The subcommittee agreed to use the edited definition.

Jennifer Schwartz of CHHS asked whether the definition of “signatory entity” includes non-state entities and wondered about the implication of applying state standards to entities that may not have the same security standards. She noted that, per the Information Practices Act (IPA), if data leaves the secure enclave, it needs to be held to the same standard as is required for GovOps.

Tom Vu of AICCU asked whether a definition is needed for “private institutions of higher education.” The document could reference Education Code 66010(b) for independent nonprofits, but a different definition may be needed for the private colleges under BPPE’s jurisdiction.

In response to a question from Stella Ngai of UC, Tom Vu of AICCU clarified that his organization would attempt to have all the AICCU members contribute data to the Cradle-to-Career Data System, which will mean that each institution will sign the data sharing agreements individually.

Bruce Yonehiro of CDE wondered whether it would be preferrable to have the independent colleges craft individual agreements specific to each data sharing instance rather than expanding the MDEA/BUCP to include non-state entities. In this way, they might be able to participate without meeting state standards.

Jennifer Schwartz of CHHS clarified that for health data, the state is mandated by the IPA to ensure any data recipients meet the SAM requirements. Ed Hudson of CSU noted that his agency has the same requirements.

Bruce Yonehiro of CDE indicated that his agency writes out security specifications that are customized based on the security structures at the receiving entity. It is up to the data provider to decide whether the data recipient has sufficient protections in place.

After considering the discussion, Tom Vu of AICCU clarified that his organization would prefer to have the MDEA/BUCP apply to independent colleges.

General Provisions

Jennifer Schwartz of CHHS raised questions about language that may be more appropriate for the BUCP, especially given that some partner entities will use the Interagency Data Exchange Agreement (IDEA) rather than MDEA as the master agreement. Also, she noted that some of the terms appear to be education specific and the meaning of these terms was unclear.

Bruce Yonehiro of CDE agreed that the language could go into the BUCP. For the terms that Jennifer Schwartz had questions about, he affirmed that these are important items for data access under FERPA, such as “authorized representative.”

Jennifer Schwartz of CHHS indicated her comments in this section could be removed, as the language states “may include” but is not required for all signers.

Next the group discussed a proposed section that allowed for stricter confidentiality and security protections. Given that the language was confusing, the subcommittee agreed not to include it.

Jennifer Schwartz of CHHS questioned a provision that states the data provider must approve confidentiality and security standards and suggested that instead all data recipients should comply with a consistent set of standards. She also reminded the group that the data will most likely be accessed through the secure data enclave.

Bruce Yonehiro of CDE agreed that this language could be deleted, so long as the data provider is informed about the security standards of the data recipient.

Jennifer Schwartz of CHHS addressed the clauses about data destruction, noting that information security experts warn that data cannot always be destroyed. Therefore, there should be qualifiers stating that in cases where data cannot be destroyed, the information should continue to be protected and only be accessed or used in alignment with the BUCP This is especially important when data providers shares information inadvertently (such as continuing to provide data after the end date of project).

Bruce Yonehiro of CDE was concerned that this language could invite parties to argue that they cannot destroy data. Stella Ngai of UC agreed, and noted that she needed confirmation from UC’s information security experts that data cannot always be destroyed.

The group edited the language in a manner that provided safeguards for un-destroyed data without making this a default position.

Jennifer Schwartz of CHHS pointed out that other language may be problematic because it appears to require data recipients to share confidential data standards with the data provider. However, this information should not be shared because it might make the system more vulnerable to a hack. Instead, she recommended that the data recipient certify they are in compliance with SAM (as is the case in the participation agreement).

Bruce Yonehiro of CDE wondered if this would be problematic for independent and private colleges and suggested that language be added instead that all data recipients conduct an annual security certification.

Ed Hudson of CSU agreed that it would not be appropriate to provide confidential security protocols, and that instead it would be better to know that the data recipient met a specific framework for security standards—however, it will be important to determine which set of standards to require. One possibility is to use the CSU approach, which requires data recipients to provide an annual attestation of an external review that says there are no material defects—this means that data recipients can follow other protocols that may be similarly rigorous but not identical.

Jennifer Schwartz of CHHS suggested that for state agencies, the agreement would mandate using a standard that is already required by the state, and allow the CSU option for non-state entities.

Ed Hudson of CSU and Mike Arakji of DGS agreed. Mike Arakji clarified that the term "attestation" may be better than "certification," based on technical requirements. He offered to write up an exhibit.

The group edited the language to address the need for an annual security attestation and documentation of security and privacy practices.

Special Terms/Security Breach Notification

Jennifer Schwartz of CHHS noted repetitious language on data recipients needing to keep data secure.

The subcommittee agreed to delete the second reference.

Jennifer Schwartz of CHHS suggested including a tighter timeframe for notification about potential breaches, given that some entities need to respond within 24 hours, not the listed 72 hours.

Ed Hudson of CSU agreed.

Mike Arakji of DGS noted that his agency uses the language "immediately, but no later than 24 hours."

Stella Ngai of UC indicated she needs to check what the required timeframe is for UC.

Ed Hudson of CSU asked what starts the clock—perhaps language should be added that specifies it is when the data recipient becomes aware an incident has occurred.

Jeannie Wolfe of CLWDA and Jennifer Schwartz of CHHS agreed. Jennifer Schwartz of CHHS further asked for clarification about what type of event would trigger the notification.

Baron Rodriguez of WestEd indicated that normally the term used is "suspected or actual breach."

Mark Paxson of CSAC indicated that HEA requires notification within one hour.

Stella Ngai of UC how much FAFSA data will be in the data system.

Kathy Booth of WestEd clarified that CSAC is providing a number of data points as noted in the P20W data set documentation. CSAC asked for changes to the trailer bill that will allow for this information to be shared under the HEA. However, other data providers will need determine whether to provide financial aid data. Currently CSU and UC have indicated that they will not share any financial aid information. Given that federal guidance about the legality of sharing information for state data sets is ambiguous, the Newsom Administration will be asking the U.S. Department of Education to provide guidance, in concert with other states including Texas and Kentucky.

Bruce Yonehiro of CDE reminded the subcommittee that the workgroup had adopted a detailed breach notification policy and protocol and suggested that the language should be consistent with those requirements.

Jennifer Schwartz of CHHS recommended that breach and incident language should be kept separate because they reflect different possible issues. For example, an incident might include information being damaged.

Mike Arakji of DGS clarified that the term “breach” may address a range of situations, for example a denial of service attack or ransomware that makes information inaccessible.

Jennifer Schwartz of CHHS argued that information security and confidentiality are different things. Lawyers think of breach as exposure of information, while information security officers think more broadly. Having separate language will make it clearer for all.

Bruce Yonehiro of CDE reflected that these are subtle distinctions, so it may be helpful to clarify what is meant in each of these scenarios. Or, the language could be combined because they have the same timeframe for a response.

Jennifer Schwartz of CHHS felt it would be burdensome to require the data recipient to alert the data provider about any possible incident.

Mike Arakji of DGS clarified that suspected incidents do not have to be reported. If it is a suspected breach, the data recipient is required to send the data provider a letter.

Carolyn Kubish of CDSS spelled out that there are three types of breach: Breach of Confidentiality, Breach of Availability, and Breach of Integrity.

Bruce Yonehiro of CDE suggested including a statement that clarifies that information is not breached if it is still encrypted, so there is no risk of improper access or disclosure.

Jennifer Schwartz of CHHS disagreed, indicating that there should be requirements to address other issues like lost or modified data.

Mike Arakji of DGS clarified that there is a gap between civil code and common terminology—for example, with ransomware attacks, the media refers to these events as breaches even though the issue is loss of access. Civil code only recognizes breaches of confidentiality and does not provide regulations regarding data availability or integrity.

The group edited the language, including providing greater clarification about data status, removing duplicative sections, and changing the assignment of language between sections.

Monique Shay of CSU asked that language be added about who is responsible for breach notification and suggested using the same wording as the BAA.

Mike Arakji of DGS felt that this would not be necessary. The incident response plan that was approved by the workgroup references the civil code section listed in the current draft.

Marion McWilliams of WestEd noted that because this agreement is between data providers and institutional members of the governing board, some data recipients may not have to comply with SAM. But if information were only provided in the secure data enclave, then the incident response would be in compliance, as GovOps would be responsible.

Bruce Yonehiro of CDE responded that breach protections are the data recipient’s obligation, even if the managing entity keeps them in compliance in the secure data enclave. Including language in the agreement would assure the data provider that the data will be treated appropriately in all circumstances. Language could be added that specifies this responsibility falls to GovOps.

Monique Shay of CSU noted that the language doesn't specify who would be responsible for notification.

Jennifer Schwartz of CHHS cautioned that no representatives of GovOps were at the meeting--they need to weigh in on this language.

The group agreed to include the suggested language, with a caveat that it should be reviewed by GovOps counsel.

Controlling Laws, Rules, And Regulations

Jennifer Schwartz of CHHS suggested adding language to clarify that parties don't need to re-execute the agreement.

The subcommittee agreed.

Security

Marion McWilliams of WestEd noted that Stella Ngai of UC added language that references SAM provisions and asked if it would be better to leave the language broader to allow for updates to security language.

Bruce Yonehiro of CDE suggested that MDEA link security to the overall standards for the Cradle-to-Career Data System and that the BUCP could include additional security standards.

Jennifer Schwartz of CHHS agreed but said additional outreach would be needed to Stella Ngai, who was no longer in the meeting.

Audit

Jennifer Schwartz of CHHS suggested edits about appropriate documentation to show the data recipient is in compliance with required security standards. Bruce Yonehiro of CDE agreed.

The subcommittee agreed to the edited language.

Signatory Language

Marion McWilliams of WestEd noted that the language was amended to clarify how additional signatories would be added to the agreement.

The subcommittee agreed with these changes.

BUCP

Bruce Yonehiro of CDE noted that there is redundant language in the BUCP about destroying personal health information.

Jennifer Schwartz of CHHS agreed it is duplicative, but clarified that state law requires this specific language be included. She reminded the group that this language will only apply to parties that are using the health data in a specific manner, which would be highly unlikely among education agencies or researchers. She recommended keeping the section separate—with language that indicates who it applies to—so that the higher burden associated with protecting health data not be triggered for other types of information.

The subcommittee agreed to not edit the language.

The subcommittee did not address suggested language about indemnification.

Next Steps

While the subcommittee finalized most edits by the end of the meeting, there was not sufficient time to canvas each member about whether they were comfortable adopting the MDEA/BUCP. Therefore, this task will be undertaken by GovOps, once the data system is under development.

Furthermore, no work was done on the participation agreement. Therefore, an additional Legal Subcommittee meeting will be held in July. A clean version of the data agreement, paired with a synopsis of foundational differences of opinion expressed in written comments from the partner entities prior to the June 29 meeting, will be shared with Legal Subcommittee members on July 8. The meeting will be scheduled during the week of July 26 to ensure that subcommittee members have time to review the document and prepare suggested edits.

After the July meeting, if any partner entity does not feel comfortable advancing the participation agreement, that agency will prepare a summary of concerns for GovOps that includes a risk assessment of not addressing those concerns. The question of how to proceed on the participation agreement will be addressed in a Governing Board meeting.

The final report to the legislature will note the draft status of the legal documents.