Legal Subcommittee Meeting Summary

May 11, 2021

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

The May 11, 2021 meeting had the following goals:

- Provide an update on key decisions from the subcommittees
- Review the proposed:
    - Incident response plan
    - Master data exchange agreement
- Discuss next steps for the participation agreement

The following representatives attended the meeting:

Veronica Villalobos Cruz, Association for Independent California Colleges and Universities; Freshta Rasoli, Bureau for Private Postsecondary Education; Kathy Lynch, California Community College Chancellor's Office; Bruce Yonehiro, California Department of Education; Marina Feehan, California Department of General Services; Kary Marshall, California Department of Technology; Cynthia (Cyndi) Bosco, California Department of Health Care Services; Carolyn Kubish, California Department of Social Services; Rima Mendez, California School Information Services; Monique Shay, Ed Sullivan, and John Walsh, California State University; Gabriel Ravel, GovOps; Jeanne Wolfe, Labor and Workforce Development Agency; Stella Ngai and Matthew Linzer, University of California, Office of the President

Update on Key Decisions by the Cradle-to-Career Workgroup

The meeting opened with Kathy Booth of WestEd providing an update on decisions made by the subcommittees at their latest meetings:

Community Engagement: Their final work will be presented at the Workgroup meeting on May 27.

Technology and Security: The Workgroup approved the Technology and Security Framework at its March 2021 meeting. The approved framework exceeds the requirements of state agencies. However, certain details will need to be completed later once: 1) Staff are hired (to identify them in the incident response plan and policy); 2) After the technology tools are procured (so that we include the correct guidelines for contractors to follow). Note that technology and security standards are continuously being updated since there are new ways that breaches can occur.

- Kathy Booth of WestEd explained that this subcommittee got as far as it could without these three details. She noted that the current Technology and Security framework meets or exceeds the policies of the Department of General Services (DGS). The legislature has approved some expenses from the remaining planning funds that will allow GovOps to hire staff. GovOps is currently working on the position descriptions and duty statements. The C2C's Executive Director will be hired through the Governing Board.
- Bruce Yonehiro of the CDE asked if GovOps would be responsible for updating data security (requires frequent updates). Additionally, he and Ed Hudson of CSU were concerned that if the

Governing Board only meets quarterly, the system would not be nimble enough to respond to threats to its security. Ed Hudson of CSU noted that this system will be the target of hackers because of the amount of data in the system. Ed Hudson of CSU also noted that the cost to the State of California for a breach is expensive ($145 per record; up to $225 per record if medical information is involved).

- Baron Rodriguez of WestEd noted that security standards, such as those from National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) are always changing. Most government agencies add requirements for third parties that require them to align their standards to the latest framework and can specify a review interval (an annual review is common). The agencies can also require an external audit (can be completed by GovOps or an outside entity) to ensure that security requirements are being kept up to date. He also noted that there could an incident response committee that is triggered when an event occurs (refer to the incident response plan noted below).
- Jennifer Schwartz of CHHS noted that the State has adopted the NIST Framework. She serves as CHHS's privacy officer, and works directly with the State's Information Security Officer. The current standards already meet or exceed HIPAA requirements.
- Bruce Yonehiro of CDE noted that even if GovOps is diligent and meets the framework requirements, there could still be a breach. He would like GovOps to have the data security expertise so they are nimble at all times. He is concerned about the liability for a breach that could cost billions of dollars and was concerned because there was push back in the draft legal agreements to require GovOps to have data security expertise.
- Gabriel Ravel of GovOps noted that hiring is in the works, and the position should be hired by the end of June or in the new fiscal year.
- Stella Ngai of UC was concerned that the Technology and Security Subcommittee was not still meeting. Kathy Booth of WestEd asked Baron Rodriguez of WestEd how close the recommendations are for what GovOps will need. He noted that a level of specificity is needed for naming roles can be easily added to the agreements. The Chief Information Security Officer is the staff designed for carrying out this plan. Baron asked Matt Linzer from UC about meeting again.
- Matt Linzer of UC noted that he would expect more maturity in the legal agreements (for tech and security issues). He and CSU have some good data sharing language that can be added and tailored to this project. The participation agreement is a good start, but not a final product yet. He would like to have CDE and CSU add their language and combine it to harmonize the requirements. There are still outstanding issues related to breach notifications. For breaches, UC requires a 72 hour notice requirement, but CSU requires 24 to 48 hours.
- Ed Hudson from CSU noted that the timeframe can be established later—but a common ground should be found. There are notification requirements back to the data contributor, the individual, the organization, the California Attorney General's office (depending on the size of the breach), etc.

Kathy Booth from WestEd noted that the Legal Subcommittee is the last committee that is still meeting. It is important to be very specific and be clear on what needs to be addressed. Please send in examples, and WestEd can send out drafts for review.

Bruce Yonehiro from CDE and Stella Ngai from UC wanted to improve the data security and incident response provisions in the participation agreement, but noted that the engagement of security experts is needed.

Kathy Booth from WestEd asked if the Technology and Security Subcommittee needs to meet again, and if so, what should be on the agenda?

Matt Linzer from UC stated that he needs to work with his legal office to see what provisions can be adjusted (and what provisions cannot be adjusted). He can bring that forward to another meeting.

Jennifer Schwartz from CHHS noted that the participation agreement needs a review by the information security officer. She thought that the participation agreement already has many of these requirements already. Adding a higher standard than necessary increases the risk that the managing entity cannot comply with the agreement (especially if there are more than one agreement to follow).

Kathy Booth from WestEd brought the group back to the process. Not everyone is aware of the procedures approved by different subcommittees. WestEd can package all legal and technology and security documents so that everyone can look at the whole package that GovOps and its subcontractors would be accountable to. Please indicate the specific sections in the participation agreement that your agency is still concerned about and bring in your technology and security representative if needed.

Bruce Yonehiro from CDE asked Gabriel Ravel of GovOps a question—Is GovOps willing to be responsible for any breach? Gabriel Ravel of GovOps stated that parties would not be indemnified.

Jeanne Wolfe of Labor and Workforce Development Agency noted that the Government Claims Act states that GovOps would be bound legally and statutorily to follow these provisions. This requirement cannot be changed in a contract or MOU. Bruce Yonehiro of CDE stated that there is a Government Code provision that allows indemnity from state agencies, but the Government Claims Act is for third parties. Bruce Yonehiro of CDE noted that he would expect GovOps to defend the claim and pay the judgment, and that this area should be handled by the Governor's Office and the legislature—it is not fair to ask the agencies to contribute data, but the agencies do not have full control. Bruce Yonehiro noted that the Governor and Legislature need to fund GovOps adequately to handle breaches—and perhaps this requirement should be addressed in statute.

Kathy Booth of WestEd noted that Marion McWilliams of WestEd will lead discussions about these issues.

Public Comment

There was no request for public comment.

Participation Agreement

Kathy Booth from WestEd noted that Marion McWilliams of WestEd will walk through the participation agreement and identify where there is work to be done, creating action items for each area. However, this work needs to be completed prior to June 30.

Marion McWilliams of WestEd described that the participation agreement (PA) is designed to be the legal agreement between the data contributors and the managing entity, setting forth a formal relationship, as required by FERPA and HIPAA. She noted that there must be specific statutory language to allow data sharing with the managing entity. The PA also identifies what the managing entity will do with the data (building the dashboards, query builder, etc.). One of the attachments contains a confidentiality and security plan.

Jennifer Schwartz of CHHS noted that the Incident Response Plan contains procedures to follow in the event of a breach. The timeline, entities involved, and responsibilities of the parties are also identified. The plan takes all of these requirements and puts these into the Incident Response Procedure. She also noted that the HIPAA Business Associate Agreement cannot be modified, due to HIPAA requirements.

Ed Hudson of CSU asked if the CISR is in alignment with the PA. Marion McWilliams of WestEd noted that CISR is standardized language, but has not been tailored to the C2C documents.

Stella Ngai from UC wanted to ensure that all requirements are included. Marion McWilliams of WestEd noted that she can review what has been drafted for data security and ensures that it aligns with the legal agreements.

Action Item for Technology and Security: Marion McWilliams noted that there is more work to be done. Are there others from the Technology and Security Subcommittee that should be invited to the homework team to finalize the language? If so, please add the names to the chat.

Type of Agreement

Marion McWilliams of WestEd led a discussion about the type of agreement the PA will be (single agreement or bilateral agreement).

Jennifer Schwartz of CHHS would prefer fewer agreements (single agreements). Additional agreements will be challenging for the managing entity to comply with. The risk is higher—delays and/or confusions. She worked with the counties on another project, and the management of each of those agreements was a big burden and they had to provide training.

Bruce Yonehiro from CDE also supported making the legal agreements easier to administer. He would like to have the group agree that the terms are the same. However, there are certain agreements that would not apply to the CDE, such as the Business Associate Agreement for HIPAA that is currently an exhibit. He was also concerned about the data elements since the partner entities need specificity about what data elements must be contributed by whom. So then do we have to set up 12 separate exhibits for the data providers? Then, if one of the entities wants to change the data elements, all 12 would have to sign an amendment. Also, if a new entity is added, then would all 12 entities would have to agree to that addition? Bruce was also concerned that any party can enforce an agreement against each other. If you have 12 parties with the same agreements with rights and obligations, that would take the CDE out of compliance with FERPA. Bruce has experience with legal agreements for a multi-state consortia.

Jennifer Schwartz of CHHS was not sure that the entities can enforce the agreement against each other. Bruce Yonehiro of CDE was supportive of a collaboration agreement, but that should be done in a separate document.

Marion McWilliams of WestEd asked the Legal Subcommittee to add issues in the chat, but to be prepared to return with specific recommendations/suggestions.

Bruce Yonehiro of CDE and Jennifer Schwartz of CHHS thought it would be helpful for Baron Rodriguez of WestEd to join the meeting.

The group then discussed who would pay if there were a data breach. Jennifer Schwartz of CHHS stated that the managing entity would send the notification to the individual and oversight entities, and would pay for any expenses. Ed Hudson of the CSU stated that alignment and agreement across all documents is needed.

Jennifer Schwartz of CHHS gave thanks to the homework team for all of their work. Marion McWilliams agreed, and noted that we are down to 3-4 major issues—we don't want to lose the energy/momentum.

ACTION ITEM: WestEd will create a list of all of the documents created for legal and technology and security.

Incident Response Plan

Marion McWilliams of WestEd noted that she will look at the other documents to check the alignment of the CISR, participation agreement, incident response plan, and the technology and security documents. She also walked the group through the incident response plan provisions. The data provider is notified, and is included as part of the incident response teams.

Matt Linzer of UC asked what laws apply for FERPA or the Information Practices Act (IPA). Gabriel Ravel from GovOps noted that both laws apply to this situation, and the IPA applies to any personally identifiable information. Julia Blair noted that noted that federal law applies to SSNs, and Stella Ngai from UC stated that the Privacy Act also applies.

Matt Linzer from UC asked about the initial loading of SSNs—will they be removed once the matching is complete, and the record assigned a unique identifier? Marion McWilliams of WestEd stated yes, and that this is an area of concern for EDD's data set.

ACTION ITEM: Members will return to the May 25 meeting with any edits.

Other Legal Agreements

Marion McWilliams of WestEd reminded the group about the Master Data Exchange Agreement. She noted that the Business Associate Agreement (BAA) needed to be attached, and how should the legal agreement clarify that the BAA is only applicable for HIPAA data?

Jennifer Schwartz from CHHS prefers that the BAA be an addendum, and not incorporated into the body of the agreement. Only two entities, the Department of Health Care Services and the managing entity would have this relationship.

Bruce mentioned that for a multi-party bilateral agreement, that we create a new FERPA authorized agreement and attach that to the participation agreement. He can work on this. He also noted that data breaches (cost of notices and credit monitoring) is a cost of the system operations. There should be a line item for GovOps to have the funds to pay for this—could include it as part of the legislation? Marion McWilliams of WestEd noted that we will follow-up with Gabriel to ask for his preference.

Next Steps

Kathy Booth of WestEd noted that several additional meetings may be needed in order to get through the remaining action items for the subcommittee. These will include:

- May 25: Continue working on completing the legal agreements (Participation Agreement, Master Data Exchange Agreement) and the Incident Response Plan and Policy. We will discuss the third-party agreements.
- June 9: Finalize all legal agreements