P20 WIN Data Security Working Group Recommendations

Overview:

The P20 WIN Data Security Working Group met between April and September 2023. The goal of the working group was to identify and create a data security questionnaire or alternative that will be required for future P20 WIN Data Requestors, as established in the P20 WIN Data Security Policy and Process.

The establishment of a data security process will help ensure that data requestors can prepare adequately to request data, that agencies can make informed decisions for the release of data, and that data are securely transmitted, stored, and released in compliance with all applicable state laws, policies, and regulations throughout the P20 WIN information lifecycle.

The following are the recommendations for review by the P20 WIN Data Governing Board:

1. The Data Governing Board should amend the Data Security Process to allow for the P20 WIN data requestors to submit a Data Security Plan as an alternative to the Data Security Questionnaire. The Data Security Plan will require data requestors to cover the same information as the Data Security Questionnaire but in a potentially more accessible format for requestors that already have a Data Security Plan prepared.
2. OPM should develop a guidebook, in consultation with security experts, with the type of Data Security documentation that will be required of requestors. This should include examples of Data Security Plans and Questionnaire responses.
3. The Data Governing Board should develop guidelines on how requestors will be provided the results as well as justification when/if the Data Security Plan/Questionnaire is rejected by a participating agency, as well as remediation suggestions to receive an approval.
4. P20 WIN should use Onspring to deploy and manage the P20 WIN Data Security Questionnaire, subject to approval from BITS.
5. Each agency should identify any “minimum requirements” that must be met by data requestors when submitting a plan/questionnaire.

These recommendations will improve the data security process, while also ensuring that the data security requirements of P20 WIN and participating agencies are documented and clear for prospective data requestors. The data security requirements of P20 WIN should be responsive to increased demands and not place a large burden on participating agencies or requestors, while ensuring the security and privacy of the data. The following section describes the process and rationale for the above recommendations.

P20 WIN Data Security Working Group Recommendations

Review of the Process:

The P20 WIN Data Security Working Group met between April and September 2023. The working group consisted of security and IT representatives from CSCU, DHMAS, DSS, UConn, OPM, and DAS/BITS. The meetings included a review of the Draft Data Security Questionnaire to identify strengths and missing questions, testing environments for the Data Security Questionnaire, deploying a pilot Data Security Questionnaire, reviewing the outcomes of the pilot, and discussing potential alternatives.

Upon reviewing the Draft Data Security Questionnaire, previously shared with the Data Governing Board, the working group created a 42-question Data Security Questionnaire covering the following areas, based on industry standard security assessments:

- Agency/Organization Information (6 Questions)
- Data Security Plan (4 Questions)
- Data Storage/Access (19 Questions)
- Data Security Training and Monitoring (10 Questions)
- Data Destruction (3 Questions)

The Data Security Working Group established the following criteria for a survey environment:

- Must allow for respondents to be able to save responses and return later to make additional edits and submit response.
- Must allow for respondents to share to others in their organizations for contributions.
- Must allow for attachments.

Upon reviewing several survey environments for the Data Security Questionnaire, including MS Forms, SurveyMonkey, JotPro, and Onspring. Onspring was identified as being the best solution for the questionnaire. Onspring is currently being piloted by DAS/BITS and meets the established criteria above.

In July, the Data Security Working Group requested five state agencies complete a pilot of the Data Security Questionnaire in Onspring. Of these agencies, four were P20 WIN participating agencies, two of which had representatives on the working group. The agency representatives were sent the link to the survey on July 21st and were given two weeks to complete the questionnaire with a deadline of August 4th. Of the five agencies, four submitted responses to the questionnaire. However, of the four agencies that submitted, only two questionnaires had complete responses, meaning the agency provided a complete response to every question, with

information that would typically be required for an agency to review a data request. The table below shows the timeline for each agency.

Agency	Link Sent	Extension Requested?	Submission Date	Completed Successfully?
Agency 1	7/21	No	7/21	No
Agency 2	7/21	Yes	8/29	**Yes**
Agency 3	7/21	No	8/3	No
Agency 4	7/21	No	8/3	**Yes**
Agency 5	7/21	Yes	NA	NA

Given the mixed results of the data security questionnaire and feedback from the agencies participating in the pilot, the working group proposes that a Data Security Plan be provided as an option for future data requestors to submit in place of completing the data security questionnaire. The working group believes this option will be more accessible for agencies or organizations that have already have a data security plan in place. For example, many researchers are already required to develop Data Security documentation or plans for research requests or institutional review board (IRB) approval. The Working Group agreed that leveraging this documentation, when available, would often provide sufficient information to assess security for a requestor. In addition, a narrative plan provides additional detail that could not be easily captured in the questionnaire format and was not reported in the pilot. The Data Security Plan will still need to address the same information covered in the Data Security Questionnaire and will be reviewed by the participating agencies that data is being requested from. Request documentation will indicate that agencies may be asked additional questions on security if topics from the questionnaire are not covered thoroughly.

Conclusion:

The list of recommendations will allow for the successful deployment of the P20 WIN Data Security Policy and Process. Both the Data Security Plan and Questionnaire options will require future requestors to address their ability securely transmit, store, analyze, and release data in compliance with all applicable state laws, policies, and regulations throughout the P20 WIN information lifecycle.

Participants:

The table below lists the individuals that devoted time and expertise to developing the questionnaire and recommendations.

P20 WIN Data Security Working Group Recommendations

Agency	Name, Title
Connecticut State Colleges and Universities (CSCU)	Peter Carey, Chief Information Systems Officer
Department of Social Services (DSS)	Jason Whelan, Chief Information Security Officer
Office of Mental Health and Addiction Services (DHMAS)	Alexander Garvey, Information Technology Subject Matter Expert
University of Connecticut (UConn)	Christopher Bernard, Chief Information Systems Security Officer
Department of Administrative Services / Bureau of Information Technology Solutions (DAS/BITS)	Justin Hickey, Deputy Chief Information Security Officer
Office of Policy and Management (OPM)	Scott Gaul, Chief Data Officer
	Coral Wonderly, Analytics Project Coordinator

Appendices 1- 3 include examples of data security plans from other state longitudinal data systems. Appendix 4 includes screenshots of the questionnaire in Onspring.

Appendix 1 – North Carolina Data Security Plan Guidelines and Sample Plan

Appendix 2 – PTAC Data Security Checklist (Used by Kentucky's KYSTATS as a guideline for writing a data security plan as part of their data request process)

Appendix 3 – Washington's ERDC Data Security Form

Appendix 4 – Onspring P20 WIN Questionnaire