Application to and Agreement with
Madison Metropolitan School District
for Releasing Data and Conducting Research upon
FORWARD MADISON

In collaboration with the Madison Metropolitan School District (MMSD), University of Wisconsin-School of Education researchers related to Forward Madison will study and report upon research to investigate the effectiveness of the Forward Madison project strands.

It has been acknowledged by ____________________________ (please print) of MMSD that the Board of Education agrees to this partnership through the MOA agreement and has approved the sharing of the data under the terms specified herein.

______________________ 3/7/16
Michael Morris Date
Contracts Coordinator
University of Wisconsin-Madison

______________________ ________
Michael G. Barry Date
Board of Education Secretary
Madison Metropolitan School District

Application to, and Agreement with, Madison Metropolitan School District for Releasing Data and Conducting Research upon FORWARD MADISON

This application and agreement are to cover the period from December 14, 2015 through December 31, 2022.

APPLICATION

1. Purpose of the research.

The instrumental purpose of the research is for evaluation of Forward Madison to inform the work of the project strand activities of induction, workforce diversity and professional learning, and the overall partnership.

2. Population for whom data are being requested.

The data requested starts with the 2014-15 school year and is inclusive of all schools and grades. Data will be provided in aggregate at the school level and disaggregated by student group, including race/ethnicity, those identified as requiring special education services, and advanced learner status.

3. Type of data requested with the specific items listed.

The data listed below will be made available to Forward Madison researchers upon request. There are two types of data potentially needed – individual-level data and aggregate by school.

Individual, student-level data

- Student demographics, including:
  - Student ID #
  - Race/ethnicity
  - Special Education services required
  - ELL status
  - Advanced learner status
- Student academic and behavior data, including:
  - Current school enrollment
  - PALS English and Espanol Grades 1-2 scores for Fall and Spring
  - MAP Grades 3-8 Reading and Math scores for Fall and Spring
  - ACT/Aspire Grades 9-11 scores
  - Out-of-School Suspensions
  - Attendance

Aggregate data

- MMSD Climate Survey data for staff, students, and parents by school
- Staff data – Year 4 Educator Effectiveness scores
- Number of TEEM Scholars hired by MMSD
- Student demographics (school level), including:
  - Race/ethnicity
  - Income
  - Special Education services required
  - ELL status
  - Advanced learner status

- Student academic and behavior data (school level), including:
  - PALS English and Espanol Grades 1-2 scores for Fall and Spring
  - MAP Grades 3-8 Reading and Math scores for Fall and Spring
  - ACT/Aspire Grades 9-11 scores
  - Out-of-School Suspensions
  - Attendance

MMSD will provide this data to the Forward Madison research team at the end of each school year through 2022. See attached Forward Madison MOA for more details.

4. **Reasons for requesting the specific data items.**

The specific data items listed above will inform the progress of implemented programming.

5. **A description of how the data will be used and analyzed.**

The data gathered will be used in evaluation and research of Forward Madison project strand activities of induction, workforce diversity, and professional learning initiatives, to inform the work of the partnership activities and specific deliverable outcomes in each project strand. These outcomes include creation of curriculum as well as meeting levels of progress as determined by both parties, i.e., educator effectiveness scores.

6. **A description of how the analysis will be presented and reported.**

Forward Madison Leadership Team will provide bi-annual updates to MMSD Board of Education, MMSD Leadership, UW-Madison and School of Education Leadership, and external funders. A first external evaluation report will be provided year end 2016. A second external evaluation report will be presented during the summer of 2017. As implementation moves to practice, project strand activities of induction, workforce diversity, and professional learning initiatives may be evaluated or researched to measure impact through 2022.

7. **Estimated amount of time the data is needed for analysis.**

The Forward Madison partnership is structured over three phases: Phase I 2014-2015; Phase II 2015-16; Phase III 2016-17. Project strand work will extend beyond this timeframe, i.e., TEEM Scholars first cohort hiring expected in 2022. Strand activities may be evaluated or researched to measure impact through 2022.

8. **Desired medium of release of the data gathered.**

Data shared will be electronically transferred to a secure, password protected University of Wisconsin-Madison Enterprise BOX account.

> Box adheres to the highest industry standards for security for sharing, accessing, and managing content with confidence. Box is also SAS70 Type II and Safe Harbor certified.

9. **Other follow-up research activities that may occur after receiving and reviewing the data.**

Matthew Hora and Sara Kraemer, of Wisconsin Center for Education Research are conducting an external evaluation of the partnership. The Forward Madison Leadership Team is also in the process of releasing a Request for Proposal (RFP) for a separate project strand evaluation. The evaluation teams will share data, program documents, and analysis as they are related to Forward Madison partnership and project strand activities of induction, workforce diversity and professional learning for evaluation purposes.

10. A plan for preventing others from viewing and using the data that addresses Confidentiality of information and Security of the system:

Data will be stored in a University of Wisconsin-Madison Box account. Box adheres to the highest industry standards for security, including:

- Content is stored on enterprise-grade servers that undergo regular audits and are monitored 24/7
- Files are backed up daily to additional facilities
- All files uploaded to Box are encrypted at rest using 256-bit AES encryption.
- For files in transit, use RC4-128 encryption, currently considered safe and secure.

11. Name and contact information of the researcher involved in day-to-day operation involving use of data, and conducting the research and analysis.

Forward Madison is under the administrative lead of the Education Outreach and Partnerships Office (EOP), UW Madison School of Education, 264 Teacher Education Building, 225 N. Mills Street, Madison, WI 53706. Principal Investigator: Beth Giles-Klinkner; Project Coordinator: Ann Halbach. External evaluation will be conducted by Matthew Hora, Research Scientist, WI Center for Education Research, 960 Ed Sciences Bldg, Madison, WI 53706. Project Strand Evaluator - TBD

12. A statement that the costs MMSD incurs in producing data will be paid by the researcher.

The Forward Madison partnership has agreed to in-kind contributions for design and implementation of programming. Research from Forward Madison will be conducted to inform program improvements.

AGREEMENT

WHEREAS the Madison Metropolitan School District (hereinafter, "MMSD") has expressed interest in engaging Board of Regents of the University of Wisconsin on behalf of University of Wisconsin-School of Education researchers related to Forward Madison, 225 N. Mills Street, Madison, WI 53706 (hereinafter "UW-Madison SOE Forward Madison researchers") to serve as an independent contractor Consultant in connection with the research of the partnership and project strand efforts toward growing, inducting and supporting educators in Madison Schools; and

WHEREAS the MMSD and UW-Madison SOE Forward Madison researchers have executed in the application and agreement section above which sets forth in detail the data sharing, data analysis and data reporting protocols, including but not limited to its purpose, scope, and duration of the research to be completed by UW-Madison SOE Forward Madison researchers on behalf of the MMSD; and

WHEREAS MMSD will share certain MMSD records with UW-Madison SOE Forward Madison researchers for the purposes of conducting the research benefitting MMSD (hereinafter referred to as the "MMSD Data"); and

WHEREAS the MMSD and UW-Madison SOE Forward Madison researchers mutually agree that the MMSD Data remains at all times the property of MMSD, and that no license or other rights to the MMSD Data is implied by the sharing of the data for the limited purpose of conducting the agreed-upon research; and

WHEREAS the MMSD and UW-Madison SOE Forward Madison researchers agree to attempt to minimize the extent to which the MMSD Data will include personally identifiable information (PII) from student records within the meaning of FERPA and/or Wisconsin Statute § 118.125 by, for example, excluding student name, student address, and student telephone number from the shared data set; and

WHEREAS the MMSD and UW-Madison SOE Forward Madison researchers recognize that it is possible that certain records within the MMSD Data, alone or in combination, may be construed as PII or as records that are otherwise protected from disclosure under state and/or federal law; and

WHEREAS, for the limited purpose of conducting the agreed-upon Forward Madison Project strand research, the MMSD has deemed UW-Madison SOE Forward Madison researchers and the individuals who are authorized representatives of Forward Madison participating in the research process to have legitimate educational interest (to wit, conducting MMSD-requested research for the purpose of improving instruction) in the records contained in the MMSD Data; and

WHEREAS the MMSD and UW-Madison SOE Forward Madison researchers intend to complete all analysis and study of the MMSD Data in compliance with state and federal laws governing the privacy and disclosure of education records and pupil records (including, but not limited to, FERPA and Wisconsin Statute § 118.125);

NOW, THEREFORE, by affixing his signature to this document, and as a condition of any potential future engagement as an independent-contractor Consultant by the MMSD in connection with research UW-Madison SOE Forward Madison researchers hereby agree to the following regarding the receipt, storage, handling, study and reporting of the MMSD Data:

1. UW-Madison SOE Forward Madison researchers receipt, storage, handling, analysis and reporting of the MMSD Data shall be conducted in a manner that does not permit the personal identification of parents or students by individuals other than (1) MMSD officials; and (2) individuals who are authorized representatives of UW-Madison SOE Forward Madison researchers who are participating in the research process and who have a need for access to the data in order to complete the agreed-upon analysis and study of the data.

2. UW-Madison SOE Forward Madison researchers receipt, storage, handling, analysis and reporting of the MMSD Data and other records received from the MMSD shall, at all times, protect and maintain the confidentiality of records to the extent required by state or federal laws or regulations or by MMSD School Board policies.

3. Any and all records within or derived from the MMSD Data shall be used only for the purpose of Forward Madison, and shall be destroyed when no longer needed for its purposes and at a date no later than 2022, unless the parties execute a written amendment hereto extending such time.

4. UW-Madison SOE Forward Madison researchers shall never re-disclose to any third-party individual, organization or entity any individually-identifiable records from the MMSD Data that are protected from disclosure under FERPA and/or Wisconsin Statute § 118.125, and shall require any authorized representative to sign a similar non-disclosure statement.

5. Except as otherwise expressly authorized in writing by the MMSD, UW-Madison SOE Forward Madison researchers shall not (1) re-disclose to any third-party individual, organization or entity any record(s) from within, or derived from, the MMSD Data; or (2) re-use the MMSD Data for any further research, study or other purpose that is not for and directly on behalf of the MMSD; (3) link the MMSD data to other data sets.

6. UW-Madison SOE Forward Madison researchers agrees to cooperate in producing any records relating to the agreed-upon research which may be subject to a request for access and/or subject to disclosure under the Wisconsin Public Records Law.

7. UW-Madison SOE Forward Madison researchers shall permit MMSD to audit, upon reasonable request, that it is complying with the Standard Security Policies and Procedures in Exhibit A and/or that it has destroyed the data as verified.

8. UW-Madison SOE Forward Madison researchers have obtained from the UW-Madison Institutional Review Board either approval or a determination of exemption for all studies conducted using Confidential Data where required by law and/or University policy.

9. If UW-Madison SOE Forward Madison researchers, individually or collectively, becomes legally compelled to disclose any MMSD Data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then UW-Madison SOE Forward Madison researchers shall use all reasonable efforts to provide MMSD with prior notice before disclosure so that MMSD may seek a protective order or other appropriate remedy to prevent the disclosure; provided, however, that UW-Madison SOE Forward Madison researchers will use all reasonable efforts to maintain the confidentiality of Confidential Data. If a protective order or other remedy is not obtained prior to when any legally compelled disclosure is required, UW-Madison SOE Forward Madison researchers will only disclose that portion of Confidential Data that it is legally required to disclosed.

10. UW-Madison SOE Forward Madison researchers acknowledge that the breach of this agreement on its part may result in irreparable and continuing damage to MMSD for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by UW-Madison SOE Forward Madison researchers, MMSD, in addition to any other rights and remedies available to it at law or in equity, may be entitled to seek preliminary and permanent injunctions, enjoining and restraining the breach or

threatened breach, and may debar UW-Madison SOE Forward Madison researchers or authorized representatives from any further access to MMSD Data.

11. ***The failure by one party to require performance of any provision shall not affect that party's right to require performance at any time thereafter, nor shall a waiver of any breach or default of this*** agreement ***constitute a waiver of any subsequent breach or default or a waiver of the provision itself. No modification, amendment, waiver or release of any provision of this agreement or of any right, obligation, claim or cause of action arising from this agreement shall be valid or binding for any purpose unless in writing and duly executed by the party against whom they are asserted.***

12. ***Any provision of this agreement that is declared invalid by a court of competent jurisdiction or by operation of law, shall not affect the validity or enforceability of any other provision of this Agreement.***

For the UW-Madison:

By signing below, the signatory represents authorization to sign this Agreement and to bind the Board of Regents of the University of Wisconsin System on behalf of UW-Madison SOE Forward Madison researchers to its terms.

3/7/16

Michael Morris Contracts Coordinator Date

For the MMSD:

By signing below, the signatory represents he is authorized to sign this Agreement and to bind the Madison Metropolitan School District to its terms.

Michael G. Barry BOE Secretary Date

EXHIBIT A

UW Box for Restricted Data – settings, guidelines, methods

This document describes security requirements that must be put in place before a UW investigator or collaborator may use UW Box for the storage of a data set containing protected health information ("PHI"). Such data set may be in the form of a limited data set ("LDS") or it may be a data set that contains direct identifiers (e.g. name, medical record number).

Ensure security of workstation.

UW investigators and collaborators that will have access to a shared UW Box folder containing PHI ("PHI Box folder") at an authorization level other than "Pre-viewer" https://kb.wisc.edu/page.php?id=37618) must access the information from a UW workstation that has met the appropriate security requirements for the data set. The UW investigator's local IT support staff must have completed all requirements, deposited an initial workstation report and deposited copies of the signed "UW Workstation Security for PHI" document, in the designated folder. (See the "UW Workstation Security for PHI processing" document for details.)

Only approved and secured workstations are allowed to be used by investigators and collaborators.

User responsibilities and requirements. Use of Box features allowed / not allowed / and other practices from protected workstations.

- Preparation:
  - Users must understand and sign the UW Workstation Security for PHI" document detailing UW-Madison requirements for workstations processing PHI.
  - Users must ensure that the workstation that they intend to use has been approved for use with PHI, by a professional IT person, per the requirements listed in the aforementioned document.
  - All users planning to work with PHI shall be fully trained via UW-Madison's HIPAA training, and have annual refresher training.
  - The principal investigator may request a PHI Box folder through their local PHI Box Agent, as described below. The Agent is often the division's HIPAA Security or Privacy Coordinator (http://www.hipaa.wisc.edu/hipaa-contact-persons.htm). Individuals in units without a designated HIPAA Security or Privacy Coordinator should contact the HIPAA Security Officer or Privacy Officer for campus.
- Use:
  - Users must access and process PHI data using only UW workstations that have been secured and approved for use with PHI.
  - Users will be allowed to create, modify and delete files and folders within their PHI Box folder based on the authorization levels requested by the principal investigator and set by the PHI Box Agent.
  - *Sharing through links:* Sharing is restricted to collaborators within the Box folder only. When sharing links, the links used must remain the randomly generated links from Box. This reduces the likelihood of a non-collaborator guessing the shared link if other security measures fail. Additionally, because sharing notifications are done through email, it reduces the likelihood that a non-collaborator with access to the email would guess that the share is related to certain PHI.
  - *Box-sync:* When an approved workstation is used, "Box sync" may be used to enhance the usability of the Box collaboration system.
  - *Box-edit:* Likewise, when an approved workstation is used, "Box edit" can be employed, which allows the use of local copies of word processing, number processing and other tools, without "Box sync." "Box edit" does cache copies of documents on the local, host disk for a period of time. (https://support.box.com/hc/en-us/articles/200521788-Box-Edit-Overview-and-FAQs#whatisboxedit).
  - *FTP to Box feature:* This **may not** be used as transmission is not encrypted.

- *"Allow upload by email":* This feature must **stay disabled** as it allows unauthenticated uploading and non-encrypted transmission.
- *Mobile devices for accessing PHI data:* Mobile devices **may not** be used to access PHI Box folders as workstation security does not allow for this.

Management of the specific UW Box PHI folders.

- Designation of PHI Box Agent(s)
  - Each division or school, desiring to offer PHI Box folders to members of their division or school, shall designate at least one PHI Box Agent for the purpose of co-owning or managing PHI Box folders.
    - Only professional IT staff, with full time appointments and trained in HIPAA shall co-own or manage folders that contain PHI. These designated PHI Box Agents must be staff with IT security background and responsibilities. Ideally, the PHI Box Agent(s) for a division or school will be the division's or school's HIPAA Security Coordinator. Other likely members include the division's or school's Madison Information Security Team (MIST) representatives, HIPAA Privacy Coordinators, CISO, or IT Director.
    - The PHI Box Agent does not need to be the local IT staff managing the security of the workstations which will be used for PHI data access and processing; the PHI Box Agent does need to coordinate with the local IT staff.
- Responsibilities
  - The local PHI Box Agent receives requests from investigators for the creation of a new PHI Box folder and forwards those requests to the UW-Madison PHI Box Folder Administrators: *Thomas.callaci@wisc.edu, konopacki@biostat.wisc.edu, stefan.wahe@wisc.edu*
  - The PHI Box Agent will reference the signed document to learn the identities of the collaborators, and learn from the principal investigator the access levels that each collaborator should receive. *Note that no investigator or collaborator is allowed to be set at an access level greater than "Editor."* (https://kb.wisc.edu/page.php?id=37618)
  - The principal investigator should be set as an Editor for the folder.
  - Important! – the PHI Box Agent must use the interactive directory tool in Box when adding UW collaborators. This ensures that their campus credentials are used for the association with this folder, even if they have other external Box accounts with UW email addresses.
  - Note that a level of Editor is required to allow the use of Box sync, thus any collaborator that is expected to utilize the box-sync tool must be set to Editor level.
  - Ensure the following settings for the properties of the PHI Box folder, which you co-own
    - General:
      - Folder name PHI_DATA-*principal investigator name-[description requested by PI]*
        - Note: Each additional study will have a new request and new folder, under the principal investigator's main folder.
      - Description – approved for *principal investigator* for use with PHI
    - Email Options
      - Do not's
        - Do not allow uploads via email
        - Do not overwrite same-name files
        - Do not disable notifications for this folder
      - Do's
        - Do send email notification at Upload and Download
    - Security (these settings are only available to owners and co-owners)
      - Do not's
        - Do not Allow people who can access this folder from a shared link to join
        - Do not hide collaborators
        - Do not Disable commenting for this folder
      - Do's
        - Do enforce "Only Owners and Co-Owners can send collaborator invites"

    - This is a key, crucial control. Triple check it.

- Accountability
    - The PHI Box Agent, in concert with the HIPAA Security Coordinator (if not the same person), shall ensure that all IT staff involved with management of the workstation, and of the PHI Box folders shall be fully trained via UW-Madison's HIPAA training (including the Security module) and must complete refresher training at least yearly.
    - The PHI Box Agent will ensure that all collaborators on the project have signed the project's "UW Workstation Security for PHI processing" document before adding an individual as a collaborator to the folder.
    - The PHI Box Agent will ensure that the workstations have been secured to the level required.

University-wide PHI Box root folder and sub folder details

Folder naming and permissions.

Folder naming and permissions as described below are used to secure the folders, reduce accidental changes and reduce accidental depositing in the wrong folders. The prepending "PHI" will reduce the burden of accounting that would be the job of the local IT staff, as collaborator reports can be searched more easily with such a tag.

- The root folder will be a UW-Box-project folder (a specific type of folder owned by the Campus Box IT staff https://kb.wisc.edu/page.php?id=36230) co-owned by the UW-Madison PHI Box Folder Administrators.
- The folder has been created and named already
    - Naming: Always prepend PHI for ease of identification.
        - PHI_*folderfunction-UDDS-abbreviation*
            - Folder functions: Reports or Data
            - UDDS is the UDDS housing the primary professor
            - Example: PHI_Data-A07-CALS
        - Subfolder – department or sub department
            - PHI_Data-A0746-NUTR_SCI
        - Next Subfolder – professor/principal investigator/other lab designation
            - PHI_Data-A0746-Lai
        - Next Subfolder – specific project
            - This is the level for adding the PHI Box Agent as the co-owner.
            - PHI_Data-Lai-2014-1539

Accounting.

The "Collaborators Report" is a Box-generated list, which includes all invited collaborators, their access level, if they are a UW "managed" or external account, dates related to invitation and acceptance, and usually includes the email of the inviter.

Box security statement (from Box, Inc.).

(https://support.box.com/hc/en-us/articles/200520608-Enhanced-Security)

Box adheres to the highest industry standards for security so you can share, access, and manage your content with confidence.

- Secure data centers: Your content is stored on enterprise-grade servers that undergo regular audits and are monitored 24/7.
- Redundancy: Files are backed up daily to additional facilities.
- All files uploaded to Box are encrypted at rest using 256-bit AES encryption.
- For files in transit, AES 256 is a supported cipher, however we default to use RC4-128 encryption. We do this to mitigate a known vulnerability in SSL called the BEAST attack, which an attacker could use to hijack someone's web session when other ciphers (including AES 256) are used. 128 bit encryption is currently considered safe and secure.

- AD/LDAP integration: Enterprise edition customers can replace Box's authentication mechanism with their own

Box is also SAS70 Type II and Safe Harbor certified.

Reviewed and accepted:

Stefan Wahe (HIPAA Security Official), *date*
Tricia Feiertag (acting UW-MSN HIPA Privacy Official), *date*