



The Association of Theological Schools The Commission on Accrediting

10 Summit Park Drive, Pittsburgh, PA 15275-1110

SENSITIVE DATA SHARING AGREEMENT FOR DATA PROVIDED BY THE ASSOCIATION OF THEOLOGICAL SCHOOLS (ATS) OR THE COMMISSION ON ACCREDITING (COA)

Individuals requesting ATS or COA sensitive data must submit the following items as a package:

- This Sensitive Data Sharing Agreement document, complete with signatures from the Investigator, Co-Investigator(s), Research Staff, and a Representative of the Receiving Institution;
- A Research Plan, as described in Section I;
- Appropriate documentation that the proposed research has been approved by the Receiving Institution's Institutional Review Board (IRB), per Section IV.F;
- A description of how data will be stored that complies with one of the three acceptable options described in Section IV.E.7; and
- A check, made payable to "The Association of Theological Schools," in the amount as outlined in Section IV.H.

The material should be sent to Deborah Gin, ATS Director of Research, 10 Summit Park Drive, Pittsburgh, PA, 15275-1110.

All requests for ATS or COA sensitive data must meet the criteria outlined in the ATS/COA "Policy on Use and Release of Data from the Institutional Database", particularly in Section II, Principles of Data Sharing. Please read the policy before completing this agreement.

I. RESEARCH PLAN

The Research Plan, no longer than two single-spaced pages, should describe the following:

- what Sensitive Data from ATS/COA are needed, including
 - parameters of the dataset
 - data source (e.g., ATS/COA database, Women in Leadership research project), if known (see list of available datasets)
 - time range in years, if longitudinal data are available
 - institutional characteristics that will be used to filter the data
- research questions (emerging or finalized) that will guide the research,
- how the data will be used (including any expected venues for dissemination).

II. DEFINITIONS

“ATS”	Association of Theological Schools
“COA”	Commission on Accrediting
“Co-Investigator”	Person with a full-time faculty-level affiliation with the Receiving Institution, in cases where the Investigator does not have such an affiliation.
“Data File”	Collection of records in any form, whether on paper, thumb drive, external hard drive, or other electronic media.
“Dataset”	Collection of raw data, with multiple cases (e.g., individuals, schools) and multiple variables (e.g., administrative role, student headcount, school’s structure); defining of datasets involves identifying the <i>type</i> of cases and specifying the <i>variables</i> being requested.
“De-identified”	At the most basic level, removal of names and titles (of individuals or organizations) for purposes of confidentiality; other forms of de-identification may include removal of variables beyond names and titles
“Digested Data”	Database information that has been collated to identify counts, frequencies, percentages, and averages (mean, median, or mode) or interpretations about the population inferred from the sample dataset (e.g., predictions, statistically significant differences) and reported most commonly in table or graph form.
“Investigator”	Person primarily responsible for analysis and other use of Sensitive Data from ATS/COA.
“Raw Data”	Non-digested information that is pulled straight from a database and most commonly provided in an Excel sheet, SPSS file, or other comma-separated value (csv) file.
“Research Staff”	All persons who are paid employees of the Receiving Institution, excluding the Investigator and Co-Investigator, who will have access to Sensitive Data from ATS/COA.
“Receiving Institution”	The higher education institution or research institution at which the Investigator will conduct research using Sensitive Data from ATS/COA.
“Representative of the Receiving Institution”	Person authorized to enter into contractual agreements on behalf of the Receiving Institution.
“Sensitive Data”	Any data from which a specific individual or school can be identified, including sets of variables that, when used in

combination, can identify an individual or school. In addition to actual identifying information (i.e., names of key informants or schools), any geographic identifiers below the level of census region, and institutional characteristics (i.e., ecclesial family, structure, and denominationality) are confidential.

“Variables”

Factors, quantities, conditions, and other characteristics that are liable to vary and that are identified for purposes of study or research.

III. UNDERTAKINGS OF ATS/COA

In consideration of the promises made in Sections IV and V below, and receipt of the monies noted in Section IV.H, the ATS/COA agrees:

- A. To notify in writing, through email, within 15 calendar days whether the request for data has been approved. Only requests consistent with the policies stated in this agreement and the principles outlined in the ATS/COA “Policy on Use and Release of Data from the Institutional Database” will be approved.
- B. If request is approved and upon receipt of this agreement properly signed by an appropriate official of the Receiving Institution and by the Investigator, Co-Investigator (if any), and Research Staff, to return to the Investigator or Designated Official by first class mail one original copy signed by the appropriate ATS/COA representative.
- C. If request is approved, to provide the Data File(s) requested by the Investigator in accordance with the description contained within the attached Research Plan, after execution of this agreement by the appropriate ATS/COA representative, and to deliver the Data Files to the Investigator via “second day” parcel service, through secure electronic data transfer, or, in some cases, email.

IV. UNDERTAKINGS OF THE INVESTIGATOR, THE CO-INVESTIGATOR, AND THE RECEIVING INSTITUTION

In consideration of the promises in Section III above, and for the use of Data File(s) from the ATS/COA, the Receiving Institution on behalf of the Investigator, Co-Investigator, and Research Staff agrees:

- A. That the Sensitive Data will be used solely for the purposes specified in the attached Research Plan.
- B. That the Sensitive Data will be used solely as described in the attached Research Plan, and that no attempt will be made to identify specific individuals or schools if such identifying

information is not included in the received dataset; nor will any listing of data at the school or individual level be published or otherwise distributed. Receiving Institution, Investigator, Co-Investigator and Research Staff agree to notify the ATS/COA, according to guidelines outlined in the ATS/COA “Policy on Use and Release of Data from the Institutional Database”, if a key informant or school is inadvertently identified or a technique for doing so is discovered.

- C. That Receiving Institution will use good faith efforts to ensure that no persons other than those identified in this agreement, or in subsequent amendments to this agreement, as Investigator, Co-Investigator, or Research Staff will be permitted access to the contents of Sensitive Data.
- D. That Receiving Institution will notify the ATS/COA of the need to provide access to Sensitive Data Files to individuals who are not Research Staff of the Receiving Institution, as defined in Section II.D above, or to collaborating institutions and agrees that the ATS/COA may require such persons to agree in writing as parties to the terms of a separate Sensitive Data Sharing Agreement. The ATS/COA retains the right to refuse sharing of data to individuals who were not named in the original approved Sensitive Data Sharing Agreement.
- E. To comply fully with the following safeguards and conditions for using Sensitive Data:
 - 1. Do not knowingly divulge any information that could be used to identify individual schools or individuals in the study and agree to use such precautions as are reasonably necessary to prevent such identification.
 - 2. Publish no tables that make it possible for a reader to identify any individual schools or individuals. No tables will be presented or published in which any cell has fewer than five responses or respondents.
 - 3. Do not attempt to contact any participating school or individual.
 - 4. If identifying information is not included in the received dataset, make no attempt to identify any school or individual in the dataset.
 - 5. Data must be backed up consistent with industry best practices to secure data. If it is necessary to print confidential data, use a printer accessible only to signatories of this agreement. Keep any confidential data that are printed or placed on non-network storage devices in a secure location accessible only to signatories of this agreement. Destroy printed material with confidential data when work is complete, but no later than one year from the date of this agreement.
 - 6. If it is necessary to use the confidential data in a room in which others are present, arrange workstations so that no one other than signatories to this agreement will be able to see confidential data.
 - 7. Handle data storage of all copies of the sensitive data in one of the following ways:
 - a. Detachable Media Storage: USB hard drives in detachable units that can be connected to a laptop or desktop computer provide a convenient and secure access method. While a USB memory key (thumb drive) can also function in this way, use

of such devices is discouraged because of the ease with which they are misplaced or stolen. However, if such devices are used, they must be encrypted.

- i. The USB hard drive/memory key must be used for storage of all original and derived datasets.
 - ii. When the data are not in use, the USB hard drive/memory key must be detached and kept in a locked storage unit.
- b. Encrypted Storage on a Local Hard Drive: Data may be kept on a local laptop or desktop hard drive if they are encrypted when not in use. This methodology requires the use of industry standard methods to encrypt original and derived data files when not in use; this approach should only be used by researchers who are familiar with this technology or who have support staff able to provide appropriate guidance.
- i. Encryption keys should be passphrase protected to ensure that keys falling into the wrong hands cannot be used to decrypt the data.
 - ii. An acceptable alternative to individual file encryption is whole-drive encryption, sometimes referred to as Full Disk Encryption (FDE) or Self-Encrypting Drives (SED), which is now being used or required at some institutions for laptop drives.
- c. Network Access: In institutional environments where secure network storage of data is provided, original and derived data files may be housed on a file server. This approach requires a pre-existing infrastructure with IT support personnel available to setup and administer the arrangement.
- i. Network access may involve directory mounts of server data to a local PC or remote logins to Linux, Unix, Mac, or Windows servers.
 - ii. Any ATS/COA sensitive data on a network must be stored in secure network locations accessible only by authorized personnel.
 - iii. Remote logins, if used, must be done over encrypted secure connections.
 - iv. The file server on which the data are stored must be physically secure and accessible only to necessary IT professional support personnel. It is assumed that the file server is appropriately patched, firewalled and monitored.
 - v. Remote (off-campus/off-site) access to network stored data must be over secured connections. VPNs are commonly used for this purpose. Under no circumstances should remote access be allowed via clear text connections.

F. That the Receiving Institution has reviewed and approved the research proposal summarized in the Research Plan under its human subjects review policies and procedures, and that a copy of the approval document has been provided to the ATS/COA. Furthermore, the Receiving Institution will maintain approval under its human subject review policies and procedures for the entire time that the Sensitive Data Files are in use.

G. That this agreement expires one year from the date of the agreement. The Receiving Institution will provide a written statement upon expiration or termination of this agreement that all copies of the Data Files in their possession have been destroyed and how

the data destruction was accomplished. Deleting data files and emptying the “recycle bin”, for example, do not meet the standards of industry best practices; rather, such best practices would include electronic “shredding” or multiple overwrites with random data. The current standard practice is to back up data multiple times a day in multiple locations, so data will likely reside on backup servers. Recognizing this, the Receiving Institution and the Investigator, Co-Investigator, and any Research Staff will never restore the data files after the contract has expired.

- H. That a non-refundable fee, in the form of a check made payable to “The Association of Theological Schools,” has been provided to the ATS/COA to cover the expenses of producing and shipping Data Files and documentation, of consulting, and of administering this agreement. (See Fee Schedule.)
- I. To respond fully and in writing within ten working days after receipt of any written inquiry from the ATS/COA regarding compliance with this agreement or the expected date of completion of work with the Sensitive Data, and to destroy Sensitive Data and provide the confirmation described in Subsection IV.G above upon written notice from an appropriate ATS/COA representative.
- J. To include in each written report or other publication based on analysis of Sensitive Data from the ATS/COA, the following statement: "Some of the data used in this analysis are derived from Sensitive Data Files of the ATS/COA, obtained under special arrangements designed to protect the anonymity of respondents. These data are not available from the authors. Persons interested in obtaining ATS/COA Sensitive Data Files should contact ATS Director of Research at research@ats.edu."
- K. To cite the source of the Sensitive Data and identify the following information in any citation in papers, chapters, or presentations, per reference style guidelines:
 - 1. Source: ATS/COA Database (or other ATS data source)
 - 2. Year
 - 3. Pittsburgh, Pennsylvania: The Commission on Accrediting/the Association of Theological Schools.
- L. To include the following disclaimer notice whenever data are reported: “Analyses and interpretations of the Commission’s data are the researcher’s and may not reflect those of the Commission on Accrediting or the Association of Theological Schools”.
- M. To send a copy of all papers or chapters produced using these data to the ATS Director of Research, at the address on this letterhead.
- N. That to the extent not prohibited by law, the Receiving Institution will indemnify and hold the ATS/COA harmless for damages incurred as a result of negligent acts in the course of this contract by Receiving Institution, including:

1. Disclosing or attempting to discover the identity of respondents (name, street address, or other information sufficient to uniquely identify an individual or school).
2. Providing unauthorized access to Sensitive Data.
3. Retaining the original or a copy of Sensitive Data after an ATS/COA request for return or destruction of the data, or after the contract period for destruction of the data, or after an Investigator certifies the destruction of the data.

The liability of the Receiving Institution applies to damages caused by any of the following:

1. the Investigator(s) and Co-Investigator(s);
 2. the Research Staff;
 3. other individuals who receive data from the Receiving Institution pursuant to this agreement or otherwise through negligence on the part of the Receiving Institution.
- O. That tort liability for acts or omissions that are also breaches of this agreement shall be governed by the law of the state of the Receiving Institution.
- P. To treat any material breach of this agreement as a potentially serious violation of the policies of the Receiving Institution, including any scientific misconduct policy, and to ensure that appropriate action is taken in accordance with Receiving Institution's appropriate policies.
- Q. That all reasonable steps must be taken to protect the confidentiality of the database as a whole and the data that are provided, and in the event of a breach of confidentiality, to notify ATS/COA in writing within 15 calendar days of knowledge of the likely breach, with a description of the extent, and potential effects, of the breach.
- R. That ATS/COA representatives shall have the right to enter the premises of the Receiving Institution for purposes of assessing compliance with this agreement at a mutually agreed date and time during normal business hours. In addition to other remedies for noncompliance provided in this agreement or otherwise under law or in equity, the Receiving Institution will be liable for the expenses of the ATS/COA for such audit if the Receiving Institution is found to be in noncompliance with this agreement.
- S. If the ATS/COA determines that this agreement has been violated, it may:
1. Prohibit any of the Investigator(s) or Co-Investigator(s) of this agreement from obtaining access to any ATS/COA Data Files.
 2. Report the violation(s) to the Receiving Institution's office responsible for conduct violations and the safeguard of confidential information.
 3. Utilize such other remedies as may be available to it under law or in equity.
- T. That the Receiving Institution has and will maintain during the term of this agreement liability and other insurance sufficient to cover their activities and obligations hereunder, including

liability resulting from breach of this agreement. The Receiving Institution shall, upon request, supply evidence of such insurance coverage to the ATS/COA.

V. UNDERTAKING OF THE CO-INVESTIGATOR

In consideration of the promises made above, the Co-Investigator agrees to assume all responsibilities of the Investigator upon written notice from the ATS/COA that the Investigator has failed to fully perform those responsibilities in accordance with the requirement of this agreement.

NAME OF RECEIVING INSTITUTION:

**REPRESENTATIVE OF THE
RECEIVING INSTITUTION:**

Signature Date

Printed Name

Title

Building Address

Street Address

City State Zip Code

ATS/COA REPRESENTATIVE:

Signature Date

Printed Name

Title

INVESTIGATORS and COINVESTIGATORS:

Signature Date

Printed name

Title

Institution

Building address

Street address

City State Zip Code

Signature Date

Printed name

Title

Institution

Building address

Street address

City State Zip Code

Signature Date

Printed name

Title

Institution

Building address

Street address

City State Zip Code

Signature Date

Printed name

Title

Institution

Building address

Street address

City State Zip Code

Research Staff:

I. The undersigned Research Staff, in consideration of their use of Sensitive Data from the ATS/COA, agree:

- A. That they have read the Sensitive Data Sharing Agreement for the ATS/COA and the attached Research Plan.
- B. That they are "Research Staff" within the meaning of the agreement.
- C. To comply fully with the terms of that agreement.

II. The undersigned Investigator agrees that the persons designated herein are Research Staff within the meaning of the associated Sensitive Data Sharing Agreement for the ATS/COA.

RESEARCH STAFF:

Signature Date

Printed Name

Institutional Affiliation

RESEARCH STAFF:

Signature Date

Printed Name

Institutional Affiliation

INVESTIGATOR:

Signature Date

Printed Name

Institutional Affiliation