AMERICAN INSTITUTES FOR RESEARCH®

Research & Evaluation – Domestic I

Development of Standardized Measure to Assess Disparate Contextual Forms of Intimate Partner Violence

Final IRB Package

JUNE 27, 2016

Submitted to:

Wendy McIntosh, MPH and Dennis Reidy, Ph.D.
Centers for Disease Control and Prevention
4770 Buford Hwy NE, MS F-63
Atlanta, GA 30341

Contract No. GS10F0112J
Order No. 200-2015-F-88061

Submitted by:

Melissa Scardaville, Ph.D., and Alison Huang, MPH
2801 Buford Highway, Suite 180
Atlanta, GA 30329-2237

Table of Contents

Screening Questionnaire

Project Abstracts, Deliverables, Security Information and IRB (PADII) Application

---

<u>For AIR Employees</u>: Please use this as a resource as you prepare for or complete your Project Abstract, Deliverables, Information Security, and IRB (PADII) Application. All information must be entered into http://padii.air.org and submitted by the Project Director before review can take place.

<u>For Collaborators</u>: Please fill out this document and return to your AIR contact. Only AIR staff have access to the PADII application and airportal.air.org links.

Yellow highlight = selected
Gray highlight = question not relevant to this study

1. What is the purpose of this IRB submission?

- ☐ **Pre-award approval.** Need an IRB review for submission of a proposal to a funding agency (The anticipated proposal submission date is: _____)
- ☐ **Provisional approval.** Seek to submit an IRB Control Form only to obtain a project number for a new project. I plan to submit materials for IRB review later.
- ☐ **Approval. (1)** Seek an IRB review for a new project or **(2)** Seek an IRB Review for a component of an existing project.
- ☐ **Approval renewal. (1)** Seek a periodic (i.e., annual) review in order to renew IRB approval. **(2)** Seek to close-out the IRB file with an IRB Final Progress Report.

2. Will the project, project task(s), or project component(s) involve any recruitment/data collection or secondary data analysis?

- ☐ Yes - The earliest anticipated recruitment/data collection or secondary data analysis start date is (If uncertain, please just give your best guess.): 09/01/2017
- ☐ No

3. Which of the following best describe this project, project task or project component? (Choose as many as apply.)

- ☐ Randomized controlled intervention study (i.e., an experiment with randomization)
- ☐ Program evaluation
- ☐ Survey work (e.g., item development, survey administration, and/or analysis of new survey data)
- ☐ Focus Groups, observations, or interviews
- ☐ Analysis of extant secondary data
- ☐ Cost or cost/effectiveness analysis
- ☐ Consulting services
- ☐ Mandatory State Assessment *(If only this option is selected, please see page 7)*
- ☐ Development of a student test or assessment (e.g., a state assessment)

- ☐ Assessment research
- ☐ Scoring student tests or assessments
- ☐ Equity analyses and support
- ☐ Usability testing or cognitive testing
- ☐ Technical assistance
- ☐ Conference planning, meeting(s) or workshop(s)
- ☐ Website or data system construction
- ☐ IRB services for external client
- ☐ Work will be performed or data will be collected outside the U.S.
- ☐ Do not know; project plans insufficiently developed
- ☐ Other: _____

4. Please describe the research plan for this project. This will help to give the IRB Reviewer some context for the review. *(Optional)*

The purpose of this survey is to increase knowledge about the factors that contribute to intimate partner violence (IPV) perpetration. This study will be a non-probability, purposive sample of 3 populations: the currently incarcerated intimate partner violence (IPV) offender population, the currently incarcerated non-IPV offender population, and the general (non-incarcerated) population. The survey will be conducted online for the general (non-incarcerated) population and in-person for the incarcerated population.

A more detailed description of the study can be found in Form A.

5. Will this project or project task involve systematic investigation that will develop or contribute to generalizable knowledge; that is, scientific or research findings or results that build on other research in the field in which this work will be done? (Please read guidance immediately below before answering.)

Please read carefully: Examples of generalizable knowledge include results that could or will be presented at scientific meetings or submitted to scholarly research journals based on results from the project. Examples of what in most cases would be non-generalizable knowledge include results from employment equity projects where personnel records collected for business purposes are analyzed for the sole purpose of advising a plaintiff or defendant in a court case, surveys developed to verify eligibility for specific client services, item development procedures for a state assessment, and forms used to evaluate a specific meeting or workshop.

Important: Projects that might not be thought of as research projects (e.g., assessment projects or demonstration projects) could include research activities that lead to generalizable knowledge. If so, check, “yes”.

- ☐ Yes
- ☐ No
- ☐ Uncertain

6. Will data from living human beings be collected as part of this project through the use of printed questionnaires, web surveys, interviews, focus groups, observations, videotaping, etc.?

- ☐ Yes
- ☐ No
- ☐ Uncertain

7. Do you plan to use human participants from any of the following populations? (Check all that apply.)

- ☐ Prisoners
- ☐ Pregnant women
- ☐ Children under 18 years of age
- ☐ Cognitively impaired children or adults
- ☐ None of the above

8. Are you collecting data on sensitive topics such as sexual behavior, HIV status, drug or alcohol use, illegal behaviors, child or physical abuse, immigration status, etc.?

- ☐ Yes
- ☐ No
- ☐ Uncertain

9. Will the data you are collecting allow you to ascertain an individual's identity? (Please read guidance immediately below before answering.)

Please read carefully: Individuals' identities can be ascertained in several ways including personal data such as names addresses, phone numbers, and identification numbers (e.g., social security and medical record numbers). In addition, audio and videotapes also enable direct identification of an individual. Finally, an individual may be identified through "deductive disclosure," that is, the ability to deduce who someone is with high probability through the cross-classification of variables such as age, gender, and employment position where sample or cell sizes are small.

- ☐ Yes
- ☐ No
- ☐ Uncertain

10. Will data be collected in a language other than English?

- ☐ Yes
- ☐ No

~~11.~~ Will non-AIR staff (e.g., temporary employees, subcontractors, recruiting firms) recruit participants or collect, analyze, or have access to data you are collecting?

- ☐ Yes
- ☐ No

~~12.~~ Are you collecting data for an education agency such as a US state, school district or school?

- ☐ Yes
- ☐ No

~~13.~~ Is your project funded wholly or in part by the National Center for Education Statistics (NCES)?

- ☐ Yes
- ☐ No

Please read carefully: NCES has very specific requirements for ensuring the security and confidentiality of any data collected on its behalf. Many of these procedures are federally-mandated and focus on those data that may enable users to identify individual respondents, either directly or indirectly through deductive disclosure or by matching to other data sources. Confidentiality procedures include, but are not limited to, a disclosure risk analysis for any data that may be released to the public, and if necessary, implementation of disclosure limitation techniques. Exact procedures will depend on the type of data being collected, and should be developed in coordination with NCES. Your IRB submission should acknowledge understanding of federal legislation with respect to NCES data, as well as your obligation to work with NCES to develop any necessary disclosure limitation procedures. See the NCES web site (http://nces.ed.gov/statprog/2002/std4_2.asp) for more information.

~~14.~~ Will you be collecting identifiable health information? Note: “Health” includes more than just physical health, but also mental, psychological, and emotional health.

- ☐ Yes
- ☐ No

~~15.~~ Will this project use existing data on humans from records, transcripts, videotapes, etc.?

- ☐ Yes
- ☐ No
- ☐ Uncertain

16. Check all that apply with regard to the type of data that will be used:

- ☐ Publicly available data on humans
- ☐ Publicly available administrative data
- ☐ Data on humans collected for other purposes that are not publicly available (e.g., data from another study that are not publicly available, personnel data)
- ☐ Administrative data that are not publicly available
- ☐ Education records (e.g., data, files, documents or other materials directly related to a student or students and maintained by an education agency or institution)
- ☐ Medical records data (e.g., from a hospital, health care provider or health insurance company)
- ☐ Other – Please describe: _____

17. Will the existing data you are using allow you to ascertain an individual's identity either directly or through the use of a code or key? (Please read guidance immediately below before answering.)

Please read carefully: Individuals' identities can be ascertained in several ways including personal data such as names addresses, phone numbers, and identification numbers (e.g., social security and medical record numbers). In addition, audio and videotapes also enable direct identification of an individual. Finally, an individual may be identified through "deductive disclosure," that is, the ability to deduce who someone is with high probability through the cross-classification of variables such as age, gender, and employment position) where sample or cell sizes are small.

- ☐ Yes
- ☐ No
- ☐ Uncertain

18. Will you be using any National Center for Education Statistics (NCES) restricted-use data (i.e., data containing individually identifiable information) for this project?

- ☐ Yes
- ☐ No

Please read carefully: Individuals must obtain a restricted-use data (RUD) license before accessing any NCES restricted-use data. Individuals apply for a restricted-use data (RUD) license from NCES through qualified institutions which have met the necessary security requirements; AIR staff may obtain a RUD license through AIR. For more information on obtaining an NCES RUD license, contact AIR's Data Security Officer. Your IRB submission should indicate that you understand procedures related to obtaining RUD licenses and ensuring the security of restricted-use data. For more information, see the NCES RUD web site: http://nces.ed.gov/statprog/instruct.asp.

19. Will non-AIR staff (e.g., temporary employees, subcontractors, recruiting firms) analyze or have access to the existing data being used in this project?

~~Yes~~

~~No~~

~~20.~~ Will the project include recording of still or video images or audio recording of participants?

Yes

No

~~21.~~ Will your project produce any outward-facing documents that will contain art such as photography, clip art, cartoons, comic strips, illustrations, audio, or video?

Yes

No

~~22.~~ Is this project classified?

Yes

No

~~23.~~ Is AIR the prime, a subcontractor, or an equal partner with another organization on this project?

Prime without subcontractors

Prime with Subcontractors

Subcontractor

Equal Partner

For AIR Employees: Please use this as a resource as you prepare for or complete your Project Abstract, Deliverables, Information Security, and IRB (PADII) Application. All information must be entered into http://padii.air.org and submitted by the Project Director before review can take place.

For Collaborators: Please fill out this document and return to your AIR contact. Only AIR staff have access to the PADII application and airportal.air.org links.

Participants

1. Please provide a detailed description of the human participants who will be involved in your project or task. These may be people from whom you will be directly collecting data and/or people about whom you will have extant data. Describe the characteristics of the population, including their anticipated number, age range, gender, and health and mental health status.

   This study will be a non-probability, purposive sample of 3 populations: the currently incarcerated intimate partner violence (IPV) offender population, the currently incarcerated non-IPV offender population, and the general (non-incarcerated) population. All participants will be at least 18 years old and live in the United States.

   We aim to collect data from 2210 respondents: 2000 general (non-incarcerated) population individuals, 105 currently incarcerated individuals who have an IPV offense record, and 105 currently incarcerated individuals who do not have an IPV offense record.

   General Population Mechanical Turk (MT) Workers: Participants from the general population will be a purposive sample of Amazon's Mechanical Turk (MT) workers. MT is a convenient, low-cost method of crowdsourcing human intelligence tasks that has been used for social science research. Individuals register as "workers" and can browse Human Intelligence Tasks (HIT) posted by "requesters." Once a MT worker successfully completes the task, they are paid through the MT interface. CDC specifically mentioned during the proposal process that use of MT was a potential source of online survey participants from the general population.

   Up to 8,600 MT workers will first complete a screening questionnaire. AIR will then choose 2,000 workers who collectively, most closely, demographically represent those of the general US population (in terms of age, sex assigned at birth, race, ethnicity, household income, and education) for invitation to complete the full survey. We will oversample individuals who identify as gay or lesbian. Studies have shown that IPV disproportionally affects this subgroup. We are oversampling to ensure that we get a large enough sample from this subgroup to achieve adequate power in our analyses. We will purposively choose participants so that our sample will be approximately:

   - Age: 14.5% ages 18-24 years, 43.1% 25-44 years, 29.0% 45-64 years, 13.4% 65 years and older
   - Sex assigned at birth: 50.8% female, 49.2% male
   - Race: 77.4% White, 13.2% Black, 1.2% American Indian or Alaska Native, 5.4% Asian, <1% Native Hawaiian and Other Pacific Islander, 2.5% Two or more races
   - Ethnicity: 17.4% Hispanic origin

- Household income: 8% Under $10,000, 6% $10,000 - $14,999, 6% $15,000 - $19,999, 6% $20,000 - $24,999, 11% $25,000 - $34,999, 14% $35,000 - $49,999, 18% $50,000-$74,999, 11% $75,000-$99,999, 20% $100,000 and over
- Education: 29.3% four year college graduate or more
- Sexual orientation: 25% men who identify as heterosexual, 25% men who identify as gay, 25% women who identify as heterosexual, 25% women who identify as lesbian.

Incarcerated Population: Participants from the incarcerated offender population will be from 1 prison and 3 work release facilities (hereinafter referred to as "facilities") in Indiana. It is expected that all individuals living in these facilities are 18 years old or older, most being between 26 and 50 years old. We anticipate about two thirds of our sample to be male. Our sample will be equally stratified by if the individual has an IPV-related offense record (e.g. charges for domestic battery). In general, this population likely has a higher proportion of individuals with health problems and mental illness compared to the general population. It is also likely that these individuals have experienced more trauma than that of the general population. Many individuals may have low literacy skills as well.

2. Identify the criteria for inclusion or exclusion of any subpopulation.

General Population Mechanical Turk (MT) Workers: Participants are eligible if they are 18 years old or older, live in the United States, are MT workers, and have a 95% or higher approval rating on their work with MT.

Incarcerated Population: Incarcerated individuals are eligible if they are at least 18 years old. All incarcerated participants must live in one of the facilities we will work with.

3. Explain the rationale for the involvement of any special classes of participants, such as children, children with disabilities, adults with disabilities, persons with mental disabilities, pregnant women, prisoners, institutionalized individuals, or others who are likely to be vulnerable. If none, write "None."

We will be surveying prisoners in 4 facilities in Indiana. We are conducting research on attitudes, conflict, and patterns of behavior, including violence, in intimate partner relationships with the goal of identifying factors that influence IPV perpetration. This data will be used for the long term goal of developing tailored perpetrator intervention programs.

Involving incarcerated IPV offenders allows us to collect data from individuals who, we can confirm through their criminal history, have actually perpetrated IPV. Ultimately (and after this contract) the data gathered from this survey will be used to develop a valid instrument to differentiate types of IPV perpetration. Some patterns of behavior, such as physical, emotional, or sexual violence, are more prevalent within the incarcerated population than within the general population. Surveying people who have an IPV offense record allows us to obtain data from a population who have likely experienced trauma, are at high risk of perpetrating IPV again, and who may have committed particularly severe or frequent offenses. The experience and personal characteristics of this population may be different from those of the non-incarcerated population and are valuable to identifying indicators that predict patterns of aggression. Additionally, it is a requirement of the funding to include incarcerated individuals in our sample.

This population is likely to have a larger proportion of individuals who are cognitively impaired or mentally unstable compared to the general population. All individuals have the option to

refuse the survey. Interviewers will be trained to recognize signs of distress and stop/pause the survey or seek help from facility staff, if necessary.

Surveying incarcerated non-IPV offenders and the general population will allow us to collect data to identify distinguishing factors between perpetrators and non-perpetrators.

Sources and Types of Data

4. Identify the sources and types of data (e.g., specimens, records, or other materials) that will be obtained or used. If the project or task is collecting or using multiple sources or types of data, indicate which will be obtained specifically for this project and which will involve the use of existing data. Similarly, if the project or task is collecting or using multiple sources or types of data, indicate the extent to which each is publicly available.

   Data will come from 3 sources: 1) IPV arrest history (has an IPV arrest on record or not) for individuals from the incarcerated population who consent to participate. Data will be provided by the facilities. 2) MT workers' responses to screening questionnaire (data collected specifically for this project), and 3) all respondents' responses to survey items (data collected specifically for this project). None of these data will be made publicly available.

5. Please attach a copy of each of your proposed data collection protocols.
   If you do not have this information at this time and will submit it later, please select "Submit Later".

   ☐ Submit Now (Attach)
   ☐ Submit Later

   See Attachment

6. You previously indicated that you will be collecting data on one or more sensitive topics (e.g. sexual behavior, HIV status, drug or alcohol use, illegal behaviors, child or physical abuse, immigration status). Please provide information about the nature of these data. (*If applicable).*

   We will ask several questions about violence that occurred within and outside of intimate partner relationships, substance use and abuse, sexual behavior, psychological conditions, attitudes that condone violence, and adverse childhood experiences. We will ask about violence that is physical, emotional, sexual, or stalking. Our expert consultants and literature review identified these areas as important and predictive factors that contribute to perpetration of IPV. It is important to understand the details of the violent occurrence(s), the reasons for violence, and personal characteristics of individuals to appropriately distinguish between IPV perpetrators and non-perpetrators and between types of IPV perpetrators. Survey items were either taken from existing scales, modified from existing scales, or written by AIR and CDC. Items were all cognitively tested with formerly incarcerated IPV offenders and non-offenders, and participants from the general population.

7. You previously indicated that you will be collecting or using data that will allow you to ascertain an individual's identity. Please provide information about the nature of these data and the extent to which they contain information such as names, addresses,

identifying numbers, photographs and video or audio recordings that could be used to identify participants. (*If applicable).* _____

General Population Mechanical Turk (MT) Workers: MT workers will participate in the survey anonymously and no identifiable information or contact information will be collected. For those who volunteer to take the survey, AIR will receive their MT WorkerID, a 14 character ID (e.g. A3IZSXSSGW80FN), which we will only use to re-contact workers who are chosen for our sample.

Incarcerated Population: AIR will not have PII associated with the incarcerated population on its systems or in hard copy outside of the facility. AIR will not be doing the sampling. The prison facility staff will be drawing a quota based sample where they select the number of inmates that meet our sampling sample size targets. When AIR staff arrive onsite, the facility would provide a list of the names of sampled inmates that AIR would meet with on that day and an indication of whether they have an IPV arrest history or not. AIR will not retain copies of lists of inmates. Each person who participates in the study will be assigned a code number. Survey answers will be associated with this code number and not the individual's name. The only form containing the individual's name is the consent form, which only researchers will have access to.

Recruitment/Consent

8. For existing data (e.g. extant data) that will be used in this project, to the extent known, please describe the recruitment and informed consent procedures used to collect the data and indicate the extent to which data confidentiality was promised to participants.

General Population MT Workers: None

Incarcerated Population: The existing data collected will be the IPV arrest history (has an IPV arrest on record or not) for incarcerated individuals who choose to participate in the study. This data will be provided to AIR by the facilities. To keep track of whether the inmate is in the IPV arrest history vs non-IPV arrest history groups, AIR would record this information in an Excel spreadsheet that has all of the AIR created code numbers generated. Once the inmate has agreed to participate and signed the consent form, they would be assigned a code number. There would be columns for IPV arrest history and non-IPV arrest history and they would be marked a '1' for the group they belong to and a '0' for the group they do not belong to. The first question in the survey will be to enter the code number. The AIR employee would enter the code number from the spreadsheet. Then the inmate would continue with the survey. The IPV arrest history information would be merged with the survey data by the code number after data collection.

9. For the data you will collect, please describe your plans for recruiting participants and the consent procedures to be followed in the text block below. In particular, spell out:
   - the circumstances under which consent will be sought and obtained;
   - who will seek it;
   - how it will be documented;
   - the nature of the information to be provided to prospective participants; and
   - information about any monetary or other incentives offered to compensate participants for research-related inconveniences.

General Population MT Workers: First, the screener survey will be posted as a simple human intelligence task (HIT) for MT workers to complete. The HIT will provide a brief description of the

screener survey, the qualifications required of MT workers for participation (at least 95% approval rating), estimated time to take the screener survey, and the reward amount (10 cents). Of those who participated in the screener survey, AIR will choose a sample to complete the full survey. These workers will be sent a request to complete a second HIT for the full survey. The HIT will again provide a brief description of the survey, the qualifications required of MT workers for participation (at least 95% approval rating), estimated time to take the survey, and the reward amount (about 3 to 5 dollars).

Sampled MT workers will be paid 3 dollars for completing the full survey and a bonus of 2 dollars if they answer at least 90% of the questions. Because this group is a worker population, the incentive scheme is designed in this way to protect AIR from receiving poor quality submissions that have only a few questions answered, while also giving participants a choice to skip sensitive questions. In justification of the incentive amounts provided to MT workers, we found that most HITs for psychology surveys and studies of family experience in young adulthood and other types of similar work provide about $0.25 for a 3-5 minute survey, $0.50 for a 5-7 minute survey and about $4-6 for a 40 to 60 minute survey. Our incentives are comparable to what other HITs offer. Previous research has shown that many MT workers do not use MT as their primary source of income and complete tasks for enjoyment or just “for something to do” that allows them to also earn money.

Both the screener survey and full survey will require respondents to read and acknowledge a consent form prior to participation. The consent form will provide information about the study purpose, who is conducting the research, how their confidentiality as a respondent will be protected, and who to contact if they have any questions about the study. Participants will be informed that the project will be receiving a Certificate of Confidentiality from CDC, which will protect the privacy of respondents by protecting research staff from being forced to release respondents’ identifying information in any civil, criminal, administrative, legislative, or other proceeding. They will be informed that their answers will be identified with a code number. Their identity will not be linked with their answers. Additionally, results from this survey will only be reported for groups of participants. Results will not be reported about specific people. We seek to waive documentation of consent for MT workers as a consent form would be the only record linking the participant to the research. If MT workers click “Agree” to the consent page on the online survey, this will be considered to be providing consent.

Incarcerated Population:

First, selected inmates will come meet with AIR staff to talk about the study and get an information sheet. Inmates who are interested in participating are invited to schedule an appointment time to complete the survey. This could be on the same day or another day. Giving the inmates time to think about if they want to participate protects the inmate’s rights to participate by not coercing them into doing the interview the first time they learn of the study. At the scheduled appointment, AIR staff will introduce the survey and review the consent form. The individual will be given the opportunity to ask any questions. The consent form will provide information about the study purpose, who is conducting the research, how their confidentiality as a respondent will be protected, and who to contact if they have any questions about the study. We will inform respondents that participation will not affect their legal case in any way, there will be no repercussions for declining to participate, and mandated reporting will occur if child abuse is disclosed. They will be informed that their answers will be assigned a code number given by AIR and their name or Facility ID number will not be linked with anything they

say. Additionally, results from this survey will only be reported for groups of participants. Results will not be reported about specific people. Individuals are required to sign the consent form if they decide to participate.

A token of appreciation in the form of a small snack (e.g. piece of fresh fruit or a candy bar) will be will be provided for participants who take the survey. The value of this incentive is attractive enough to be a reward for participants but small enough to not be coercive.

~~10.~~ Please upload a copy of your proposed recruitment materials and consent form (and/or related documents such as consent "information sheets" or cover letters). A Word version of the informed consent checklist can be found here.

If you do not have this information at this time and will submit it later, or you are requesting a waiver or alteration of consent and thus do not have any applicable materials, please select "Submit Later".

- ☐ Submit Now (Attach)
- ☐ Submit Later

~~11.~~ Please indicate if you are requesting any of the following (Select all that apply):

- ☐ A waiver of **documentation** of consent
- ☐ A waiver or alteration of consent *(These are rare)*
- ☐ A waiver or partial waiver of HIPAA authorization *(These are rare. Please complete FORM E: HIPAA)*
- ☐ None

~~12.~~ Waiver of **documentation** of consent (if selected above)

- ☐ Yes (Please indicate how your study meets each of the criteria necessary for the IRB to grant a waiver of documentation of consent: _____)
- ☐ No

When an IRB has not waived the requirement for seeking prospective informed consent of the subjects or the parental permission of children who are subjects, it may waive the requirement for a signed consent form for some or all subjects if it finds EITHER:

- that the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality (e.g., the only thing that would link a human subject to a study of persons who are HIV positive is a consent form)…. or
- ~~that the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context (e.g., drawing blood, asking shoppers in a mall about ambient lighting or temperature).~~

~~13. Waiver or alteration of consent (if selected above)~~

~~☐ Yes (Please indicate how your study meets each of the criteria necessary for the IRB to grant a waiver or alteration of consent: _____)~~

~~☐ No~~

~~An IRB may waive or alter the requirements of informed consent provided that ALL of the following four conditions are met:~~

- ~~the research involves no more than minimal risk to the subjects;~~
- ~~the waiver or alteration will not adversely affect the rights and welfare of the subjects;~~
- ~~the research could not practicably be carried out without the waiver or alteration; and~~
- ~~whenever appropriate, the subjects be provided with additional pertinent information after participation.~~

~~(Note: "Practicable" is not an inconvenience or increase in time or expense to the investigator or investigation, rather it is for instances in which the additional cost would make the research prohibitively expensive or where the identification and contact of a large number of potential subjects, while not impossible, may not be feasible for the anticipated results of the study.)~~

Risks/Benefits and Risk/Benefit Analysis

~~14.~~ Describe potential risks (physical, psychological, social, legal, or other) to participants and assess their likelihood and seriousness. Describe potential benefits to participants (health-related, psychosocial, or other) or others (such as acquisition of generalizable knowledge). Where appropriate, describe alternfCAative treatments and procedures that might be advantageous to the participants. Discuss why the risks to participants are reasonable in relation to the anticipated benefits to participants and in relation to the importance of the knowledge that may reasonably be expected to result.

Some questions might be uncomfortable or embarrassing to answer for participants. The benefits to participation are that participants will help contribute to the body of knowledge about IPV perpetration, which may help to create more effective and tailored perpetration intervention programs. This study is one step towards helping to prevent intimate partner violence in the future.

General Population MT Workers: If there was a breach in confidentiality and workers' identities were released, their answers to the survey could cause problems with their job or personal relationships. There is also a risk of individuals revealing something that is potentially incriminating to themselves when answering questions about illegal activities. The survey also asks several sensitive questions which may be psychologically and emotionally difficult for respondents.

Incarcerated Population: The participants' identity could be discovered through deduction if data about their names, Facility ID, facility, criminal history, and sex were released. If the participants' identify was discovered and answers or comments were shared in connection with their name, this could cause problems with their job or personal relationships. There is also a risk of individuals revealing something that is potentially incriminating to themselves when answering questions about illegal activities. The survey also asks several sensitive questions which may be psychologically and emotionally difficult for respondents.

Protections for Participants

15. Describe the procedures for protecting against or minimizing potential risks to participants (including risk of physical harm and risks arising from breaches of confidentiality such as harassment, ostracism, psychological harm, civil liability, criminal prosecution, loss of employability and financial loss), and assess their likely effectiveness. Where appropriate, discuss provisions for ensuring necessary medical or professional intervention in the event of adverse effects to the participants. Also, where appropriate, describe the provisions for monitoring the data collected to ensure the safety of the participants. Note that Project Directors are responsible for insuring that all project staff have completed appropriate training regarding the protection of human participants. Information about staff who have and have not completed accepted training may be obtained from the IRB Administrator (IRBAdministrator@air.org). If any IRB reviews will be conducted at any partner organizations, please include information about this here._

We will inform participants that if they disclose information that leads us to believe there is child abuse or elder/disabled abuse occurring, we are mandated by law to report this to authorities.

General population MT workers: The participant will have the opportunity to pause the survey and will be provided clear instructions on how to end the survey, if desired. If possible, a pop up will be programmed to appear to ask if the participant if they are OK if they remain on a question for a certain period of time. Contact information for help lines or support organizations will be provided at several points during the survey.

MT workers are given an overall approval rating based on the quality of their work they submit. If a worker submits work that is rejected by the requester, their approval rating will go down. MT workers will be informed that, if they consent to take the survey, they will receive 3 dollars for taking the survey and a bonus of 5 dollars if they complete at least 90% of the questions. They are able to skip any questions or stop the survey at any time and will still receive 3 dollars. Skipping questions or stopping the survey will not affect their approval rating in any way.

All data will be temporarily stored on the survey software's secure server and will be securely transferred to a FISMA compliant server for storage. The online survey software's servers, databases, and web presences will be HIPAA compliant and employ multiple forms of security features. Their security protocols are designed to protect the data as well as the confidentiality of research participants.

Incarcerated population: Participants will be informed that they may refuse to answer any questions or stop the interview without penalty. Surveys will be conducted individually in a private, quiet room. Because the survey topic is sensitive in nature, interviewers will be trained to recognize signs of distress and will be instructed to ask participants if they are OK and pause/stop the interview if needed. Participants will also be given information about who to go to within the facility if they need support.

Participants might feel uncomfortable if facility staff know who chooses to participate in the survey. They may feel like they have to participate or else they will be punished. In the information sheet and when the study is introduced, we will stress that participation is voluntary and that there are no repercussions for not participating. Only essential facility staff will know that we are conducting a survey. Non-essential staff will only be informed that some inmates have an appointment. They will not know the purpose of the appointment nor the fact that inmates were able to choose to participate or not. Additionally, we will have a memorandum of

understanding (MOU) in place to address roles and responsibilities of facility staff, especially in regard to confidentiality.

The consent form will be the only document that contains the inmates' names. All paper consent forms will be stored in a secure, locked, location. No personally identifiable information will be included in the survey data file. Participants will only be identified by a code number. Researchers will not have access to the list inmates who participate in the study after data collection is complete. The survey data collected through the survey software will be stored on the software's secure server. Data will be uploaded to the survey software servers daily, or as soon as possible, and taken off of the iPad. The online survey software's servers, databases, and web presences will be HIPAA compliant and employ multiple forms of security features. Their security protocols are designed to protect the data as well as the confidentiality of research participants. After data collection, data will then be transferred to a FISMA compliant server for storage. AIR staff will be in possession of the iPads and monitor their use at all times. All iPads will be password protected and stored in locked storage containers when not in use. At night, iPads will be stored in a locked, secure location at AIR's Indianapolis office.

Furthermore, during informed consent and at the conclusion of the appointment, inmates will be given information about available resources within the facility should they need support after participation in the survey. Some survey questions may be triggering and prisoners might need mental health resources after. Inmates may also need support if they want to discuss the survey or their participation after AIR interviewers have left the facilities.

~~16.~~ Please list key personnel for this project:

The IRB will not be able to issue an approval for your work until you and all of your key personnel have completed training in the protection of human research participants. AIR policy and the terms of our Federalwide Assurance state that staff who collect or analyze data from living humans must complete training in the protection of human research participants. Key personnel who have not completed the training will receive an email notifying them to do so. Certificates of completion can be uploaded into PADII via the "Check My Certification" link on the left dashboard.

Melissa Scardaville
HarmoniJoie Noel
Alison Huang
Roger Jarjoura
Nathan Zaugg
Konrad Haight

Screener Survey Consent Form
Consent Form: MT General Population Sample

What is this survey about? What will you ask me to do?
This is a screener survey to collect demographic information from some Mechanical Turk workers. We will ask you to answer questions about yourself. If your background matches the needs of our survey, we will send you another Human Intelligence Task (HIT) directly. The HIT will be a request to complete a full survey about problems in relationships between intimate partners.

This screener survey will take about 5 minutes. You will receive 10 cents for doing the screener survey. If your background matches the needs for our full survey, you will receive up to 5 dollars for taking the full survey.

Who is conducting the screener survey?
The American Institutes for Research (AIR) is conducting this survey. AIR is a research organization based in Washington, DC. The survey is funded by the Centers for Disease Control and Prevention (CDC), a government agency.

Do I have to take the screener survey?
No. It is your choice whether to do the screener survey or not. If you decide to do the screener survey, you can stop taking it at any time. You do not have to answer any questions that you don't want to. There are no penalties and your approval rating will not be affected if you decide to skip any questions, if you do not complete the screener, or if you chose to start the screener survey and change your mind later.

What are the risks and benefits if I take the screener survey?
There are few risks to taking the screener survey. You may feel uncomfortable answering some of the questions on the survey. You may, skip questions that you are uncomfortable answering or stop taking the survey at any time.

The benefits to taking the screener survey are that if your background matches the needs of our full survey, you will have the chance to earn up to 5 dollars for completing the full survey in another HIT.

How will you protect my privacy?
We know how important it is to keep your information private. We will take all steps to keep your information confidential. Your answers will only be identified by a code number given to you by AIR. Your WorkerID, which will only be used to send you the next HIT if you are eligible, is only known by project team researchers. Your WorkerID will not be linked with any of your answers. Additionally, results from this screener survey will only be reported for groups of participants. We will never report results about specific people.

What if I want more information?

If you have additional questions or concerns about this survey, please contact the director of the survey at AIR, Melissa Scardaville, Ph.D. at (404) 260-1046.

If you have concerns or questions about your rights as a participant, contact AIR's Institutional Review Board (which is responsible for the protection of people taking this survey) toll free at 1-800-634-0797 or c/o IRB, 1000 Thomas Jefferson Street, NW, Washington, DC 20007.

Please click the "Agree" button if you agree to take the screener survey
Clicking the "agree" button means that you are agreeing to take this screener survey. This means that you have read and understood the information on this form and you are willing to take the survey under the conditions we described.

Screener Survey
MT General Population Sample

1. What is your age?

_____ years

2. What sex were you assigned at birth, on your original birth certificate?

0 ☐ Male
1 ☐ Female

3. Which of the following best represents how you think of yourself?

0 ☐ Gay (lesbian or gay)
1 ☐ Straight, that is, not gay or lesbian
2 ☐ Bisexual
3 ☐ Something else
4 ☐ I don't know the answer

4. What is the highest grade or level of school that you have completed?

0 ☐ 8th grade or less
1 ☐ Some high school, but did not graduate
2 ☐ High school graduate or GED
3 ☐ Some college or 2-year degree
4 ☐ 4-year college graduate
5 ☐ More than 4-year college degree

5. What was your total household income during the past 12 months?

0 ☐ Less than $10,000
1 ☐ $10,000 to $14,999
2 ☐ $15,000 to $24,999
3 ☐ $25,000 to $34,999
4 ☐ $35,000 to $49,999
5 ☐ $50,000 to $74,999
6 ☐ $75,000 to $99,999
7 ☐ $100,000 to $149,999
8 ☐ $150,000 to $199,999

9 ☐ $200,000 or more

6. Are you Hispanic or Latino?

0 ☐ No

1 ☐ Yes

7. What is your race? *Mark one or more*.

0 ☐ White

1 ☐ Black or African American

2 ☐ Native Hawaiian or Other Pacific Islander

3 ☐ Asian

4 ☐ American Indian or Alaska Native

Understanding Relationship Dynamics and Conflict Survey

Consent Form-Incarcerated Population

Thank you for coming today. Please read (or ask me to read) the information below about our survey. Be sure to ask if you have any questions. If you are willing to take part in the survey, please sign your name at the bottom and give the form back to us.

What is this survey about? What will you ask me to do?
This survey is about problems and violence that sometimes happen in relationships between partners, such as boyfriends and girlfriends or husbands and wives. We will ask you to answer questions about yourself and your relationships.

You are one of about 2,210 people taking this survey. Everything we learn will help us think about ways to understand violence in relationships.

This survey will take about 75 minutes. You are welcome to help yourself to one of the snacks we have here.

Who is giving the survey?
The American Institutes for Research (AIR) is giving this survey. AIR is a research organization based in Washington, DC. The survey is funded by the Centers for Disease Control and Prevention (CDC), a government agency.

Do I have to take the survey?
No. It is your choice whether to do the survey or not. If you decide to start the survey, you can stop taking it at any time. You do not have to answer any questions that you don't want to. There are no penalties or punishments if you choose not to take the survey. There are no penalties or punishments if you chose to take the survey and change your mind later.

What are the risks if I take the survey?
You may feel uncomfortable answering some of the questions on the survey. Remember, you can, at any time, skip questions that you are uncomfortable answering or stop taking the survey.

Some questions ask about your thoughts, experiences, or past illegal activities, including violence towards other people. We know that if other people found out about your answers, it can be embarrassing or cause problems in your relationships. Please know that anything you share will be kept private and never linked to your name.

There is one exception. If you share information about child abuse or abuse of an elderly or disabled person that is currently happening, we must report this to the proper

authorities. We will not ask you to tell us about this and we suggest that you do **not** share this information during the survey.

What are the benefits if I take the survey?
Please know that taking this survey will not affect your case. It will neither help nor hurt your case in any way.

The benefits to taking the survey are that you will help add to what is known about violence in relationships. This could help form better programs that address relationship violence.

How will you protect my privacy?
We know how important it is to keep your information private. We are taking all steps to keep your information confidential. This informed consent statement is the only form that will carry your name. This form will be stored in a secure location away from any other study files related to you. Only the research team will have access to these forms.

If you decide to take the survey, your survey answers will be anonymous. This means we will not include your name on your survey. Instead, we will assign your survey answers a code number. Prison or facility staff will not know this code number and they will not have access to your survey answers. Researchers will know whose names match with these numbers only on days they are administering the survey to people in your facility. Your name will not be recorded in connection to your survey answers or the code number.

The survey will be administered in this facility and thus we must comply with the rules of the institution. For example, you may be escorted to the room where we are giving the survey by a facility staff member, and we cannot control whether this room will be monitored in some way by facility staff. However we will not share any survey answers with facility staff, and survey answers will not be connected to participant's names. Your privacy will be protected to the extent possible within the rules of the institution.

Your survey answers will be stored in a computer file in a secured location along with the answers of everyone else participating in this study. Only the research team will have access to this file. Your assigned code number, not your name, will be the only identifier in this file. We will only report information from this study with all the answers grouped together. That is, we will describe how many participants gave one particular answer versus another. We will never report results about specific people.

What if I want more information?
Please ask us today if you have any questions. If you have additional questions or concerns about this survey, please contact the director of the survey at AIR, Melissa Scardaville, Ph.D. at (404) 260-1046 or 2801 Buford Highway, NE, Atlanta, GA 30329.

If you have concerns or questions about your rights as a participant, contact AIR's Institutional Review Board (which is responsible for the protection of people taking this survey) toll free at 1-800-634-0797 or c/o IRB, 1000 Thomas Jefferson Street, NW, Washington, DC 20007. Your counselor can help you get in touch with these resources, if needed.

Signature of Subject or Legally Authorized Representative
I have read (or someone has read to me) the above information. I have been given the chance to ask questions, and my questions have been answered to my satisfaction. I have been given a copy of this form.

If you agree to take the survey, please put a check mark next to the statement below along with your signature and the date to indicate that you agree to participate in this survey.

___ I agree to take the survey

Your signature:_____ Date:_____

Print your name:_____ Appointment time:_____

Understanding Relationship Dynamics and Conflict Survey

Consent Form-MT Population

What is this survey about? What will you ask me to do?
This survey is about problems and violence that sometimes happen in relationships between intimate partners. We will ask you to answer questions about yourself and your relationships.

You are one of about 2,210 people taking this survey. Everything we learn will help us think about ways to prevent violence in relationships.

This survey will take about 50 minutes. You will receive 3 dollars for doing the survey and a bonus of 2 dollars if you answer at least 90% of the questions.

Who is conducting the survey?
The American Institutes for Research (AIR) is conducting this survey. AIR is a research organization based in Washington, DC. The survey is funded by the Centers for Disease Control and Prevention (CDC), a government agency.

Do I have to take the survey?
No. It is your choice whether to do the survey or not. If you decide to do the survey, you can stop taking it at any time. You do not have to answer any questions that you don't want to. There are no penalties and your approval rating will not be affected if you decide to skip any questions. There are no penalties and your approval rating will not be affected if you chose to start the survey and change your mind later.

What are the risks if I take the survey?
You may feel uncomfortable answering some of the questions on the survey. Remember, you can, at any time, skip questions that you are uncomfortable answering or stop taking the survey.

Some questions ask about your thoughts, experiences, or past illegal activities, including violence towards other people. We know that if other people found out about your answers, it can be embarrassing or cause problems with your job or in your relationships. Please know that anything you share will be kept private and never linked to your name.

What are the benefits if I take the survey?
The benefits to taking the survey are that you will help add to what is known about violence in relationships. This could help form better programs to prevent relationship violence.

How will you protect my privacy?

We know how important it is to keep your information private. We will take all steps to keep your information confidential. Your answers will only be identified by a code number given to you by AIR. Your WorkerID, which was only used to send you the Human Intelligence Task (HIT), is only known by project team researchers. Your WorkerID will not be linked with any of your answers. Additionally, results from this survey will only be reported for groups of participants. We will never report results about specific people.

What if I want more information?
If you have additional questions or concerns about this survey, please contact the director of the survey at AIR, Melissa Scardaville, Ph.D. at (404) 260-1046.

If you have concerns or questions about your rights as a participant, contact AIR's Institutional Review Board (which is responsible for the protection of people taking this survey) toll free at 1-800-634-0797 or c/o IRB, 1000 Thomas Jefferson Street, NW, Washington, DC 20007.

Please click the "Agree" button if you agree to take the survey
Clicking the "agree" button means that you are agreeing to take this survey. This means that you have read and understood the information on this form and you are willing to take the survey under the conditions we described.

AIR Project Information Security Plan Form

1. Introduction and Administration: The purpose of the Information Security Plan Form is to define the user-oriented information security measures and procedures to protect project data that contains personally identifiable information. See Here for instructions on completing this form.

Project Name or Project Number	CDC IPV Metric
Project Director/ designated staff responsible for overseeing the execution of this security plan	Melissa Scardaville
Project Director review date (last review date)	July 26, 2016

2. Applicable External or Client Security Requirements (list by name below):

Data must be stored using a FISMA compliant servers.

3. Determination of Data Security Category: List the data types that will comprise the research work and security categories for each data type in the table below. See the AIR Security Categorization Intranet page for additional guidance in determining the proper security category for various data type. ***(The table below must be reviewed by the PD prior to submission due to its importance and the downstream processes associated with different security categories.)***

	Brief Description of Each Data Type [Example Input Here]	**Security Category**
3	**General Population Screener Survey**: This file will include Amazon's Mechanical Turk worker's responses to demographic questions. Respondents will only be identified by a WorkerID number. No contact information will be collected.	Low
4	**Mechanical Turk (MT) WorkerID:** This file contains the WorkerIDs for those who completed the screener survey. This file will be used to re-contact workers who are chosen from the sample. Respondents will only be identified by a WorkerID number.	Low
5	**Raw Survey Data**: This file will include all respondents' responses to the survey. Respondents will only be identified by an ID number given to them by AIR. No contact information will be collected.	Low
6	**Clean Survey Data:** This file is a cleaned version of the raw survey data, which includes all respondents' responses to the survey. Respondents will only be identified by an ID number. No contact information will be collected.	Low

4. User Environment

- **Location of Users** [Example Input Here]
  (x) AIR office(s):__Georgetown, Atlanta, Indianapolis_____
  ( ) Home
  ( ) External Organization: _____
- **Estimation of Number of AIR Personnel Accessing Data**: __6___

5. Description of AIR Security Safeguards and Procedures: Below is a listing of user-level security safeguards and operating procedures that will be employed during the various phases of the project. A listing of the key system controls managed by AIR IT are located in Tab A of this security plan.

A. ADMINISTRATIVE

1. Assignment of Security Responsibility: The Project Director (PD) is responsible for ensuring all AIR employees, contractors, and consultants working on the project comply with the security measures described in this security plan.

2. Confidentiality Agreements: The PD (or designate) will insure Non-Disclosure Agreements for sensitive information to include support contractors, consultants, and relevant IT staff are executed and filed prior to data access.

3. Reporting of Security Breaches: All staff shall be aware of their duties to report breaches or suspicious activities in accordance with internal AIR procedures (report to PD, IT/Chief Information Security Officer) as soon as possible after observation of the breach.

4. Confidentiality of Human Participants: The PD will ensure that all project staff has completed appropriate training regarding the protection of human participants. The project staff, with guidance from the Institutional Review Board, have planned numerous steps to protect the confidentiality of human participants that are described in the "Form A" of the PADII submission (internal AIR process). Details of how human participants are protected via data security measures are described throughout this plan.

B. ACCESS CONTROL

1. Need to Know: Access to project electronic data files, email, hard media, recordings, portable media, and hard copy paper files/print outs must be controlled based on a "need to know" basis determined by the PD. The assignment/removal of access to systems/electronic folders, not administered by the project (e.g., shared work folders), will be performed by the IT Department (AIR IT Service Desk).

2. Termination of Access: System access to data will be terminated for voluntarily separated personnel as soon as possible; access for involuntarily separated personnel shall be revoked immediately (in coordination with HR; HR will generally be responsible for notifying IT).

3. Periodic Audit of Access Controls: The PD will ensure that Windows file folders permissions, used to control access to sensitive data (e.g., data determined to have security category of either MODERATE or HIGH), are audited at least quarterly to ensure that only project personnel with the continued "need to know" are the only individuals permitted access to this data.

4. System Access Controls: See Tab A for description of key network/system access controls.

C. TRANSFERRING PROJECT DATA TO/FROM EXTERNAL ORGANIZATIONS/PERSONS

1. Complete Table below for Data that is shared or transferred between organizations (e.g., AIR and external party) [Example Input Here]

Data Type **(From Section 3 above)**	**Sending Organization**	**Receiving Organization**	**Type File Sharing** (Enter no. below)
MTurk WorkerIDs	Mechanical Turk	AIR	8 – using open source software (CRAN-R and MTurkR)
Clean Survey Data	AIR	CDC	Surgeon General Report project server

Types of File Transfer/Sharing (edit as needed):

1 - AIR Secure FTP (SFTP) is projected to be used to transfer files
2 - AIR Secure web portal/SharePoint is projected to be used to transfer/share files
3 - AIR inSync file sharing (Druva)
4 - External organization hosted file sharing/transfer
5 - Email (see section C2. Below)
6 - Mail (non-electronic) (see section C2. Below)
7 – Hand Carry/courier service
8 - Not known at this time

2. AIR confidentiality measures associated with the transport of data having security categories of either MODERATE or HIGH are listed below:

Email:

- Employ encryption to secure email (attachments) that is supported by AIR IT (and if necessary the external party depending on solution). (See "Encryption" in Tab A for AIR supported encryption)
- Passwords/passphrases used to encrypt/decrypt files need to be exchanged with the external party separately from the encrypted data. Passwords/passphrases as a minimum must meet the AIR password standard. (See "Password Standard" in Tab A)

Mail (non-electronic)**:**

- For shipments of sensitive portable media, see section D.4 (Portable Storage) below for proper security measures that need to be enabled prior to shipment.
- Use shipping options that employ tracking pickup, receipt, transfer and delivery of shipments (e.g., FedEx, Certified Mail, Registered Mail, Express Mail, DHL or licensed and bonded courier services).
- No obvious external markings or information identifying the contents inside shall be written, stamped, or otherwise inscribed on the packing material.
- For the mailing of hard copy sensitive individually identifiable Information (PII), attempts will be made to avoid transferring multiple direct identifiers in the same shipment.

D. STORING PROJECT DATA

1. **Hard Copy:**
   - The storage of hard copy documents, tapes, or other physical media, that includes identifiable or other sensitive project data will be stored in a lockable container inside a lockable office under the control of the PD (or designated personnel).
   - Sensitive printouts will be secured at all times during the printing process. Printouts will be sent to only printers that incorporate access control or printers that can be directly observed by a user who has access to the data.
2. **Crosswalk files**
   - Both hard copy and electronic Crosswalk files that map individual identifiable data to a de-identified code shall be stored in a separate folder/container from data required for research purposes. Access to crosswalk files shall be further compartmented and limited to only those personnel determined by the PD.
3. **User "Endpoint" Computing Systems** (Desktops, laptops, tablet computers, smart phones/handhelds, etc):
   - User computers used to access network resources are considered secondary storage areas when not possible/practical to connect to the primary data storage area (e.g., mobile environment prevents access).
   - The storage of sensitive personal identifiers any endpoint computing system hard drives are not authorized unless this data is encrypted with an AIR-approved encryption application
   - The user systems are projected to be **[Please select item that applies]**:

     ( ) AIR-issued desktops
     ( ) AIR-issued mobile computing devices (e.g., iPad/iPhone, BlackBerry)
     (x) AIR-issued laptops with disk encryption*(e.g., Windows 7 laptop with PGP Whole Disk Encryption)
     ( ) AIR-issued laptops without disk encryption
     ( ) Other: _____

     ** Contact the CISO (number below in section 8) or IT Service Desk if you do not know what disk encryption is or how to recognize it on an AIR system*
4. **Portable Storage [Please select item that applies]** (e.g., portable storage not including laptops such as external USB storage, flash drives, DVD/CDs, digital recording devices, etc):

   (x) Portable storage is projected to be used to store non-identifiable data (e.g., data determined to have security category of LOW). All devices should be secured in lockable containers when not in the physical possession of the user.
   - iPads will be used for data collection in facilities. Data collection will occur offline and will be uploaded to the survey software server (and taken off the iPad) at the end of each day. Thus, survey data will be temporarily stored on the iPad. iPads will be password protected and always in possession of or monitored by the interviewer when in use. When not in use, iPads will be stored in locked storage containers.

( ) Portable storage is projected to be used to store identifiable data (security category of either MODERATE or HIGH). **AIR required confidentiality measures listed below:**

- Personal storage devices are not authorized for the store of research data
- Storage device or files stored on it shall be protected using either disk or file level encryption supported by AIR IT. (See "Encryption" in Tab A for AIR supported encryption)
- Passwords/passphrases used to encrypt/decrypt files or provide access to the device as a minimum must meet the AIR password standard. (See "Password and PIN Standard" in Tab A)

( ) Digital video/audio recording devices are projected to be used to store identifiable data: **AIR required confidentiality measures listed below:**

- For video/audio recording devices that do not support password /pin protection, disk encryption, or file encryption is an option, then the only reasonable security control is to maintain strict physical access control (remain on person or stored in lockable storage when not under direct observation).
- For devices that permit PIN access, as minimum employ 4 digits that do not include predictable, repeating or sequential numbers. (See "Password and PIN standard" in Tab A)
- Transfer data from recording device to AIR system as soon a practical, and then delete data on recording device.

5. **Enterprise Server Storage:**

- The primary storage area for electronic project files is physically located in either a data center or secure server room. The server system(s) projected to be employed are: [Example Input Here]

( ) Internal file server (e.g., H drive if at 1000TJ) or AIR managed SharePoint. Please enter data below:

Windows Network Share (full path)	
AIR SharePoint Location	

() High Security Category data (e.g., EPHI, sensitive PII with direct personal identifiers)

All HIGH data that includes EPHI or other sensitive PII that includes direct personal identifiers (e.g., SSN) shall be encrypted in all storage states that include both online storage and backups. The AIR solution to protect the storage of files on AIR files servers (network project folders) is "Symantec File Share Encryption" (previously "PGP NetShare"). The data will only be accessible by those users who have PGP Whole Disk Encryption configured on their AIR system (see Action Item 3 in section 7 below). The encrypted folder designated to secure this data is indicated below (enter "same as above" if same folder as indicated in item above)

Windows Network Share (full path)	

( ) Separate dedicated project Server on AIR managed network:

Server Name	
Network Share/Drive path	

(x) Other:

Service Name	Surgeon General Report project server
Description of files	MT Worker IDs, General Population Screener survey data, Raw Survey Data, Clean Survey will be stored here.

6. **Online Survey Tools:** *[skip this section if no survey tools are planned]*

- The below survey tool is projected to be used for this project:

( ) AIR hosted, Vovici EFM Continuum (AIR license – multiple Programs)
( ) AIR hosted, Vovici 6, Enterprise (EHDW managed license)
( ) AIR hosted, REDCap
( ) External online survey tool. Please enter tool below:

(x) Other. Please enter tool below:
DatStat Illume or Unicom Intelligence
( ) Unknown at this time

- All response data will be transferred from the server to the designated project storage area at the completion of the survey (or as soon after as practical) or when the data is no longer needed on the server.

The data will be transferred from the survey software to staff desktops and then uploaded to the Surgeon General Report project server.

7. **Internet Web Site:**

( ) There will be a public-facing web site developed for this project (by AIR developers) that will be used to access/store sensitive data (does not apply to AIR managed Internet-facing SharePoint).

E. MEDIA PROTECTION

1. **Media/Data Retention. AIR required confidentiality measures listed below:**
   - Data owned/provided by external party (e.g., secondary extant data) will be disposed of as per data agreement between AIR and the other party.
   - Audio/video recordings will be destroyed as soon as possible when no longer needed by the project (e.g., after transcription or as per other client agreements)

2. **Marking and labels. AIR required confidentiality measure listed below:**
   - **LOW Security Category Data:** The PD should use of classification markings for documents that are transferred outside of the standard working environment where the likelihood of accidental sharing to unauthorized persons is higher.
   - **MODERATE OR HIGH security Category Data:**

     Electronic Media (e.g., email, electronic documents, removable media): To mitigate the unauthorized disclosure of PII and other high-risk data, classification markings/ labels** will be employed to properly identify the contents and ensure proper handling of the data.

     Hard Copy: Classification/control markings and/or disclaimers will be used for hard copy paper documents, memos, and reports.

   ***Consult with the AIR Data Classification Intranet page for definitions of classification levels used at AIR and guidance on the use of classification markings/label. Client-mandated email/fax disclaimers will likely be found in the project contract/SOW.*

3. **Sanitization and Destruction. AIR required confidentiality measures listed below:**
   - **LOW Security Category Data**: Destroyed at the discretion of the PD
   - **MODERATE OR HIGH security Category Data:**

     Hard copy media will be destroyed by a cross cut or diamond cut shredder shall be used to ensure proper destruction beyond reconstruction/recognition. The AIR shredding service (containers are located in common work areas), may be used for high bulk requirements.

     The PD will notify IT if there are special sanitization or destruction requirements as per project contract security requirements or data agreements.

6. Additional Security Measures (if needed):

We will have a Memorandum of Understanding with all prisons and work release facilities.

7. Action Items:

(x) 1. The project will coordinate with the IT Service Desk a request to set up a project folder restricted to only those personnel working on the project (if one is not already configured with proper permissions).

( ) 2. The project will coordinate with the IT Service Desk to configure SFTP service.

( ) 3. Symantec File Share Encryption Related Action Items (reference section 5.D.5. above):

( ) a. The project will coordinate with the IT Service Desk to configure Symantec File Share Encryption on designated file share(s) to be accessible to only personnel with the need to access this data (from endpoints with their assigned PGP Keys)

( ) b. The project will coordinate with the IT Service Desk to have them configure object level access auditing on the designated encrypted file share (to record when, who, what related to files accessed in the designated folder)

( ) **c.** The project will coordinate with the IT Service Desk to re-install PGP WDE on existing user desktops to secure access to the Symantec File Share Encryption installed on designated file share(s) (this is contingent for users that needs access to the encrypted file share from their assigned desktop instead of or in addition to their laptop that has PGP WDE)

( ) 4. The project will coordinate with the IT Service Desk regarding the purchase/installation of encryption software not already installed on the desktop/laptop.

( ) 5. The project will coordinate with the IT Service Desk for purchase of NIST FIPS 140-2 L3 validated (256-bit AES encryption) USB devices. Recommend Model: Ironkey™ Basic S250 USB Flash Drive (in either 2GB, 4GB, and higher capacities). IronKeys (made by Imation) can be purchased from PC Connection or other IT approved vendor.

(X) 6. The project will coordinate with the IT Service Desk to set up a space on the Surgeon General Report project server for this project.

8. Security Contact Information:

Role	Name	Phone/Email
Project Security Representative	Melissa Scardaville	404-260-1046
AIR Chief Information Security Officer	Robert McMahon, Sr.	202.403.5777
IT Enterprise Architecture & Engineering	Cory Schultheis	650.843.8180
AIR Education Unit Data Management (Chicago or Naperville Research Data)	Shaheen Khan	630.649.6585

9. References

1. IRB Information Security Planning section of the CISO Intranet site (AIR internal link)
2. DMS-SOP005, Protection of Research Data, LPA Data Management (AIR internal link)
3. AIR Information Security Policy (AIR internal link)
4. AIR Proprietary Information Policy (AIR Internal Link)
5. AIR Use of Information and Communications Technologies Policy (AIR internal link)
6. AIR Password Standard and Procedures Summary (AIR internal link)
7. AIR Data Classification Policy (AIR internal link)

10. Document History

Date	Document History Log	Author/Editor
6/8/16	Original security plan created	Huang, Alison
1/27/17	Update with new plan so AIR does not have PII in its possession.	Noel, HarmoniJoie

Tab A – System and Application Controls (For Reference Only)

Below are the system controls generally in place for any AIR managed system:

<table>
<tr><th>Control Type</th><th>Security Protective Measure Description</th></tr>
<tr><td>Network/System Access (stored on servers)</td><td>- Access to project information on shared network drives, Microsoft SharePoint, databases, and other information systems are generally controlled using Active Directory role-based access control (e.g., network access to Microsoft resources) or local file/folder permissions (e.g., across all operating systems).
- Coordination between data owner/system manager and IT will be made to ensure user and Group level permissions are controlled based on principle of least privilege access model.</td></tr>
<tr><td>Password and PIN Standard</td><td>- Access to project data will require “unique” user IDs in accordance with AIR Password strength standards summarized below (reference AIR Password Policy):
<table>
<tr><th colspan="2">Password/Pass Phrases</th></tr>
<tr><td>Minimum Length</td><td>12 characters (standard user)
20 characters (privileged user)
32 characters (service accounts)</td></tr>
<tr><td>Character requirements - (3 of 4 required)</td><td>Min. 1 upper case character
Min. 1 lower case character
Min. 1 number
Min. 1 special character (@, #, %, etc.)</td></tr>
<tr><td>Maximum Age</td><td>90 days (standard user)
60 days (privileged user)</td></tr>
<tr><td>Account lockout</td><td>Corporate user account (e.g., laptops, desktops) lockout occurs after 10 bad attempts within 15 minutes. After 10th attempt, lockout duration is 20 minutes</td></tr>
<tr><th colspan="2">PINs</th></tr>
<tr><td>Minimum Length</td><td>4 digits</td></tr>
<tr><td>Character requirements (all 3 are required)</td><td>No repeating numbers (e.g., 1111, 222, 9999,etc)
No ascending/descending numbers (e.g., 0123, 2345, 6789, etc)
No numbers based on information people may already have or easily obtain (e.g., your birthday, office number, phone number, address, etc.)</td></tr>
</table></td></tr>
<tr><td>Endpoint Screensaver Settings</td><td>
<table>
<tr><th colspan="2">Screensaver Settings (set via Domain group policy)</th></tr>
<tr><td>Standard setting</td><td>30 minutes</td></tr>
<tr><td>Privileged user</td><td>15 minutes</td></tr>
<tr><td>HIPAA</td><td>3 minutes</td></tr>
<tr><td>Federal Restricted Use Data</td><td>5 minutes</td></tr>
</table></td></tr>
<tr><td>Encryption</td><td>The following applications are supported by AIR for encrypting data:
File encryption applications and supported algorithms)
- Microsoft Office 2007 (or newer) applications (128-bit AES encryption)
- WinZip versions 10.x or newer (128-bit or 256-bit AES encryption)
- Adobe Acrobat versions 9x or newer (256-bit AES encryption); versions 7 and 8 (128-bit AES encryption)
- PGP Zip on AIR computers (256-bit AES encryption)
Disk/Volume encryption (AES)
- Symantec PGP Whole Disk Encryption (WDE)
- Microsoft BitLocker volume level encryption (for Microsoft OS)
- FileVault II volume encryption (for MacOS)
Network Folder
_ - Symantec File Share Encryption
Other File Protections:
- File-level password protection mechanisms found in older Microsoft Office applications are note suitable as a security measure.
- Worksheet level password protections found in Excel are not designed to be secure and should not be used to provide confidentiality (e.g., hidden columns in Excel can be readily seen using other word processing applications).</td></tr>
<tr><td>Remote Access</td><td>- Network access from external users:
-- IPSec VPN (restricted to AIR provided laptop and properly configured certificate)</td></tr>
</table>

	-- Web SSL VPN (from any web browser) -- Windows Terminal Server (from Windows RDC or IE web browser)
Physical Access Controls to AIR Data Centers	- Physical access to network file servers and database servers that store project data are in AIR IT data centers are restricted to only IT personnel and key facility managers using proximity badge access controls where badge use is electronically logged to a central system. - The physical space inside AIR data centers/server rooms are monitored with video surveillance - A visitor access log is maintained to manually log all personnel who do not have badge access
Perimeter Security	- All business/project data is protected by at least one commercial-grade firewall - AIR IT/Web Services employs a commercial-grade intrusion prevention system in addition to commercial-grade firewall
Security Patches and Upgrades	The security systems administrator shall ensure that security patches and upgrades released by the respective manufacturers of the components of the information assets used to process all data are promptly applied to the components.
Malware Protection	- All desktops, laptops, and servers that store data employ malware protection - Automated updating of virus signatures
Data Backup and Replication	- At least once per 24 hrs - Disk-to-disk or disk-to tape - Offsite Storage of Tape Media: weekly, monthly, quarterly and semi-annual tapes are picked up be secure courier once per week and stored at secure offsite location - Windows CIFS from all AIR locations are replicated to internal offsite AIR data center
Security Logging	- All Windows Domain servers and endpoints are configured with Windows security event logging as per audit policy (Windows Security, Application and System logs)
Sanitization and Destruction	- Physical Destruction: All IT managed storage hardware designated for disposal (e.g., hard drives, printers, magnetic media) is physically destroyed by AIR's recycling vendor by shredding the hardware to guaranty 100% destruction of all data. Smaller bulk sensitive optical media (e.g., CD/DVD) can also be physically destroyed via document cross-cut shredding devices. - Sanitization: Hard drives that include sensitive data that are designated for re-use by IT are sanitized IAW DoD 5220.22 standard . - A "Certificate of Data Destruction" will be provided to the project or client upon request

AIR Institutional Review Board (IRB)
Form E: To Be Used Where HIPAA May Apply

<u>For AIR Employees</u>: Please use this as a resource as you prepare for or complete your Project Abstract, Deliverables, Information Security, and IRB (PADII) Application. All information must be entered into http://padii.air.org and submitted by the Project Director before review can take place.

<u>For Collaborators</u>: Please fill out this document and return to your AIR contact. Only AIR staff have access to the PADII application and airportal.air.org links.

Whenever a project uses extant medical or health insurance records, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) may apply. The Privacy Rule and the Security Rules for the protection of individually identifiable health information are pertinent to AIR projects. **Please carefully read the sections below and answer the questions that follow to determine how HIPAA affects your project and what kind of IRB review is required.**

HIPAA and the Standards for Privacy
In response to a congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the U.S. Department of Health and Human Services (HHS) issued the regulations Standards for Privacy of Individually Identifiable Health Information . For most covered entities, compliance with these regulations, known as the Privacy Rule, was required as of April 14, 2003.

HIPAA and the Standards for Security
The HIPAA Security Rule provides administrative, physical, and technical safeguards for protecting electronic protected health information (EPHI). EPHI is any PHI that is created, stored, transmitted, received or disposed of in electronic format.

The final Security Rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003 and became effective April 20, 2005. Like the Privacy Rule, the Security Rule applies to covered entities. However, the obligations imposed by the Security Rule may also apply to those who receive EPHI from covered entities in accordance with a BAA or DUA.

The Security Rule describes how to implement administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of EPHI.

> ***Confidentiality*** is the assurance that EPHI data is shared only among authorized persons or organizations.
>
> ***Integrity*** is the assurance that EPHI data is not changed unless an alteration is known, required, documented, validated and authoritatively approved. It is an assurance that the information is authentic and complete, and that the information can be relied upon to be sufficiently accurate for its purpose.
>
> ***Availability*** is the assurance that systems responsible for delivering, storing and processing of EPHI data are accessible when needed and by those who need it both during normal operations and during a business disruption/emergencies.

EPHI is any PHI that is created, stored, transmitted, received or disposed of in electronic format.

Identifiable Health Information Excluded from HIPAA

Education Records: The definition of PHI under HIPAA specifically excludes identifiable health information in "education records" subject to the Family Education Rights and Privacy Act (FERPA, 20 USC 1232g). FERPA provides privacy protections for such records when held by federally funded educational institutions. See FERPA Intranet page of this website for additional information.

- **Employment Records:** The definition of PHI under HIPAA also excludes employment records for covered entities for activities related to their employment function. However, in their health roles, they create records containing what is defined as PHI for any employees for whom they provide health services. Refer to http://privacy.med.miami.edu/glossary/xd_employment_records.htm for additional information related to this exclusion.

Comparison of the HIPAA Privacy and Security Rules

The Privacy Rule focuses on the right of an individual to control the use of his or her personal information. It covers the confidentiality of PHI in any form or medium including electronic, paper and oral. Confidentiality is an assurance that the information will be safeguarded from unauthorized disclosure. The physical security of PHI in all formats is an element of the Privacy Rule. The Privacy Rule is enforced by the Office for Civil Rights of the Department of Health and Human Services (HHS).

The Security Rule focuses on administrative, technical and physical safeguards specifically as they relate to electronically protected health information. The Security Rule has more specific and comprehensive security controls than those specified in the Privacy Rule for electronic data. Protection of EPHI data from unauthorized access, whether external or internal, stored or in transit, is all part of the HIPAA Security Rule. The Centers for Medicare & Medicaid Services (CMS) has been delegated authority to enforce the non-privacy provisions of the HIPAA Regulations, including the HIPAA Security Rule.

Relevance to AIR Projects

HIPAA applies to the use of PHI by covered entities for treatment and payment. AIR is not a covered entity, but is responsible for meeting the covered entity's obligations under the HIPAA Privacy and Security Rules when it receives PHI from a covered entity to conduct projects. HIPAA applies to both research and non-research projects conducted by AIR.

Non-Research Projects

When AIR contracts with a covered entity to conduct non-research work that requires access to PHI, AIR enters into a Business Associate Agreement with the covered entity. The BAA specifies AIR's obligations to adhere to the terms of the Privacy and Security Rules. For example, if AIR contracts with a health insurer to conduct a direct social marketing campaign that informs its members about weight control, the insurer must reveal to AIR the names of its beneficiaries. Health insurance enrollment information is PHI because it is used to pay claims. Because the insurer is contracting with AIR to conduct a normal business operation, it will require AIR to enter into a BAA before releasing the data.

Research Projects

Research organizations are not themselves covered entities, unless they are also health care providers and engage in any of the covered electronic transactions. Researchers, who are not workforce members of covered entities, may be indirectly affected by the Privacy Rule if covered entities supply their data. When AIR needs to acquire PHI to conduct research, it enters into a Data Use Agreement with the covered entity that agrees to provide the PHI. This might be the client, another organization. The DUA specifies the uses to which AIR may put the data, the actions it will take to protect the privacy and security of the data, and actions it will take to inform the covered entity supplying the data in the event of a breach of privacy or security. For example, if AIR is surveying Medicare beneficiaries for CMS as part of a research project, and samples from a list of Medicare beneficiaries supplied by CMS, it must enter into a DUA, because CMS is a covered entity. If the project requires PHI from hospitals, AIR must enter into a DUA with each hospital that agrees to provide the PHI. Because research is not a normal business operation, the DUA, rather than the BAA, is the appropriate agreement.

Important PHI Definitions

1. PHI includes any of the following 18 data items in electronic, paper, or oral form:

    - Names
    - Geographic subdivisions smaller than state
    - Dates more specific than year
    - Telephone numbers
    - FAX numbers
    - Email addresses
    - Social Security Numbers
    - Medical Record Numbers
    - Health Plan beneficiary numbers
    - Account numbers
    - Certificate/license numbers
    - Vehicle identifiers
    - Device identifiers
    - Web URLs
    - IP addresses
    - Biometric identifiers such as finger or voice prints
    - Full face photograph or image
    - Any other number, code or characteristic that can be linked to identity ***by the researcher.***

2. A “de-identified data set” cannot contain ANY of these 18 data items.

3. A “limited data set” may not contain the above 18 data items, except for dates more specific than the year and location more specific than the state; note that street name, street number, and P.O. Box number may not be included in a limited data set, but county or zip code can be included.

Use and Disclosure of PHI for Research

The Privacy Rule permits covered entities to use or disclose PHI for research purposes either with an individual's specific written permission, termed an “Authorization,” or without it, if certain conditions are met. A covered entity is permitted to use or disclose PHI for research purposes if one of the following conditions is met:

- Obtains the individual's Authorization for the research use or disclosure of PHI as specified under section 164.508 of the Privacy Rule.
- Obtains satisfactory documentation of an Institutional Review Board (IRB) or Privacy Board waiver of the Authorization requirement that satisfies section 164.512(i) of the Privacy Rule. To grant a waiver, the IRB or Privacy Board must find that the research meets all of the following conditions:

    - No more than minimal risk;
    - Adequate plan to protect identifiers;
    - Adequate plan to destroy identifiers ASAP;
    - Written assurances that PHI will not be disclosed for purposes other than approved;
    - Research could not practicably be conducted without the waiver;
    - Research could not practicably be conducted without using PHI ;
    - Waiver will not adversely affect rights or welfare of subjects; and
    - When appropriate, subjects will be provided information later.

  The covered entity supplying the data and the researcher receiving the data must enter into a Data Use Agreement (DUA) specifying how these conditions have been met.

- Obtains satisfactory documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual.
- Uses or discloses PHI for reviews preparatory to research with representations from the researcher that satisfy section 164.512(i)(1)(ii) of the Privacy Rule (e.g., to review medical records to determine if research is feasible).
- Uses or discloses PHI for research solely on decedents' PHI with representations from the researcher that satisfy section 164.512(i)(1)(iii) of the Privacy Rule.
- Provides a limited data set and enters into a Data Use Agreement with the recipient as specified under section 164.514(e) of the Privacy Rule.
- Uses or discloses information that is de-identified in accordance with the standards set by the Privacy Rule at section 164.514(a)-(c) (in which case, the health information is no longer PHI).
- Uses or discloses PHI based on a permission that predates the applicable compliance date of the Privacy Rule (generally, April 14, 2003), i.e., an express legal permission to use or disclose the information for the research, an informed consent of the individual to participate in the research, or a waiver by an IRB of informed consent to participate in the research. See the Privacy Rule at section 164.532(c).

The Common Rule and HIPAA have similar, but somewhat different requirements for privacy, confidential, and security. For example, procedures that are considered adequate to protect confidentiality under the Common Rule may not be adequate under the HIPAA Privacy and Security Rules. The definition of a “de-identified” data set under HIPAA differs from the definition of an “anonymous” data set under the

Common Rule. Thus, a project that is exempt under the Common Rule because the data are anonymous may require a waiver of authorization under HIPAA because the data are not de-identified.

For a more detailed explanation about research and the Privacy Rule and for more information about the various sections referred to above, please visit the government's official website for the following document on the use of PHI for research: http://www.hhs.gov/ocr/hipaa/guidelines/research.pdf. You might also want to visit: http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp, a site from which much of the information here was drawn.

The specific standards and implementation procedures related to the Security Rule safeguarding EPHI also can be located on AIR's intranet here: http://airportal.air.org/Services/CSO/Web%20Pages/HIPAA%20Security.aspx. Included in this website are useful references and links that should provide additional background related to implementation of the Security Rule.

1. Except for the exclusions noted above (employment and/or education records), will this project or task use Protected Health Information (PHI) or Electronic Protected Health Information (EPHI)?

   - ☐ Yes, this project will collect EPHI
   - ☐ Yes, this project will collect PHI (non-electronic)
   - ☐ Yes, this project will collect both EPHI and PHI
   - ☐ No
   - ☐ Unsure (Please describe the nature of your data and indicate why you are unsure if it is PHI or not:_____)

2. Since you are using EPHI, a written information security plan needs to be developed. Please upload a plan for ensuring the confidentiality and security of the information you will be collecting and/or using. For plan preparation, please refer to the below link that provides specific guidelines and helpful templates on developing an information security plan that includes security measures associated with accessing, storing, and transmitting data. (http://airportal.air.org/services/cso/Web%20Pages/IRB.aspx)

   It is recommended that you develop your data security plan in coordination with the AIR Chief Security Officer and/or IT Data Security Officer (IRBSecurity@air.org), as they will be notified when you upload your plan and asked to approve it.

   - ☐ Submit now (Attach)
   - ☐ Submit later

   *Security plan will be attached

3. Since you are using identifiable health information, a written information security plan needs to be developed. Please upload a plan for ensuring the confidentiality and security of the information you will be collecting and/or using. For plan preparation, please refer to

the below link that provides specific guidelines along with a helpful template on developing an information security plan that includes security measures associated with protecting PHI. (http://airportal.air.org/services/cso/Web%20Pages/IRB.aspx)

☐ Submit now (Attach)

☐ Submit later

4. Which of the following actions are you requesting from the IRB?

☐ Approval to obtain the individual's authorization for the research use or disclosure of PHI as specified under section 164.508 of the Privacy Rule.

☐ Approval of a waiver of the individual's authorization requirement and the use of a DUA that satisfies section 164.512(i) of the Privacy Rule. (Attach)

☐ Approval to alter the Authorization requirement and obtain altered Authorization from the individual.

☐ Approval to use or disclose PHI for reviews preparatory to research under section 164.512(i)(1)(ii) of the Privacy Rule.

☐ Approval to use or disclose decedents' PHI for research under section 164.512(i)(1)(iii) of the Privacy Rule.

☐ Approval to use a limited data set and a DUA under section 164.514(e) of the Privacy Rule.

☐ Approval to use or disclose information that is de-identified in accordance with the standards set by the Privacy Rule at section 164.514(a)-(c) (in which case, the health information is no longer PHI).

☐ Approval to use or disclose PHI based on a permission that predates the applicable compliance date of the Privacy Rule (generally, April 14, 2003).

Updated 5.19.2010