HSR Protocol Cover Sheet

UVA Study Tracking Number:

HSR Submission Number: 12351

Title: Effect of Opiate Reduction on Clinical Outcomes and Hospital Cost in Neonates Undergoing Abdominal Surgery

IRB Review Type: Exempt

Principal Investigator: Jeffrey Gander , MD
(434) 243-4267
jg9br@virginia.edu
Box: Box 800709
School of Medicine, Surgery

Study Coordinator I: Rachel Simon , RN, BSN
(434) 243-7653
rmg5r@virginia.edu
Box: 801370

IRB Coordinator: Rachel Simon , RN, BSN
(434) 243-7653
rmg5r@virginia.edu
Box: 801370

Scientific Contact: N/A

Administrative Contact: Rachel Simon
rmg5r@virginia.edu
(434)243-7653
Box: 801370

Sub-Investigators:

David Grabski , MD	School of Medicine, Surgery
Rick Vavolizza	School of Medicine, Medicine

Additional Study Coordinators:

Sponsor(s): N/A

Funding Grant(s): N/A

Five Year Update: NO

Location of Study:

PRC Study: NO

IND N/A

IDE: N/A

Auxiliary Documents Required for Submission:	• Data Security Plan
If applicable, submit one copy of any other you have such as:	• Questionnaires • Surveys • Manual of Operations • Package Inserts

Auxiliary Documents Required for Approval:	None
Other Documents:	NONE

Committee Conflict: NONE

Question/Answers for HSR Submission: 12351		
1.	Is this protocol funded by an external grant?	NO
4.	Do you or will you have a contract with an outside entity to fund this protocol OR to share data with anyone not listed on the protocol, other than sponsor or CRO, prior to publication?	NO
10.	Is there an entity inside of UVA supporting this study?	NO
11.	Will this study be submitted through the PI's current primary school and department appointment?	YES
12.	Is this a single site Collaborative Analysis study in which data from this study being done by UVa personnel will be combined with data from other sites conducting the same or similar study?	NO
14.	Is this a multi-site study?	NO
18.	Will data/specimens be collected at another institution such as another health system, a school or HealthSouth and sent to UVA?	NO
19.	Is this a 5 year update of a previously approved protocol?	NO
20.	Will you collect data from the Clinical Data Repository (CDR)?	NO
21.	Will this study involve any of the following? • Collection (e.g., blood drawing) and/or processing of a specimen*(e.g., anything that involves the specimen container to be opened) AT UVA occur OUTSIDE of a UVA clinic/hospital or clinical lab such as in a research lab • Use of recombinant or synthetic nucleic acid molecules, gene transfer/therapy, biological vectors or infectious agents	NO
22.	Does the study involve any of the following items that will require approval of the study from the Institutional Biosafety Committee?	NO
23.	Will any of your data involve information about students governed by the federal FERPA regulations, such as information from Student Health, the Registrar's Office, the Office of Assessment and Studies, or the Student Information System (SIS)?	NO
24.	Will you do any of the following in this study? • Collect or store IDENTIFIABLE* data onto ** an individual use device*** • Collect or store IDENTIFIABLE data via web based format (e.g., online consent, online surveys) via a non-UVa server. Only exception is sharing or storing of data by sponsor or CRO in which data will be sent and stored in an encrypted fashion (e.g. Secure FX, Secure FTP, HTTPS, PGP). • Collect or store to a server NOT included in the list of HIPAA compliant servers****	NO
25.	Will the research involve UVA medical residents or fellows as subjects?	NO
26.	Will the research involve UVA medical students as subjects?	NO
27.	Will the study require Expedited or Full Board review?	NO
86.	Do you ONLY plan to do research with data previously collected as part of an Improvement Project (e.g. Performance Improvement, Practice Improvement, Quality Improvement) in which there was no interaction or intervention with an individual and the project only involved the use of information from UVa medical records?	NO
88.	Does this study meet Exempt approval criteria?	YES

TEMPLATE SECTIONS
EXEMPT APPLICATION
DATA SECURITY PLAN

UNIVERSITY *of* VIRGINIA

Office of the Vice President for Research
Institutional Review Board for Health Sciences Research

Confirmation of Training in Human Subject Protection

HSR # : 20324 **Title :** Effect of Opiate Reduction on Clinical Outcomes and Hospital Cost in Neonates Undergoing Abdominal Surgery

This is a certificate confirming that the following personnel have completed University of Virginia Research Training, an on-line tutorial that reviews the core concepts for the responsible conduct of research in a way that is consistent with federal and university requirements. Following each topic summary, the investigator must correctly answer the test question before being allowed to continue. This training is required every three years.

Name	Training	Last Trained	Expires
Rachel Simon	HSR	(HSR CITI - Update) 04-Oct-16	04-Oct-19
Jeffrey W Gander	HSR	(HSR CITI - All Researchers) 31-Aug-17	31-Aug-20
Rick D Vavolizza	HSR	(HSR CITI - All Researchers) 25-Sep-17	25-Sep-20
David Grabski	HSR	(HSR CITI - All Researchers) 14-Sep-17	13-Sep-20

11/29/2017

Richard Stevenson, MD — Date
Chair, Institutional Review Board for Health Sciences Research (UVA IRB)

One Morton Drive, Suite 400 • P.O. Box 800483 • Charlottesville, VA 22908-0483
434-924-2620 • Fax: 434-924-2932
www.virginia.edu/vprgs/irb/

EXEMPT APPLICATION FORM

INSTRUCTIONS AND INFORMATION

Enter responses electronically. Email this completed form and the Protocol Cover Sheet to IRBHSR@virginia.edu for pre-review. DO NOT SUBMIT in PDF FORMAT. An IRB staff member will reply with any changes to be made.

This project will NOT qualify for exempt approval if you plan to collect health information AND if:

1. *You need to link data/specimens from more than one source. (Go back into Protocol Builder and answer NO to the exempt question and follow further instructions provided by Protocol Builder.)*
2. *Data/ specimens being sent or received are identifiable. (Go back into Protocol Builder and answer NO to the exempt question and follow further instructions provided by Protocol Builder.)*

IRB-HSR Submission #:12351 ***(Found on first page of Protocol Cover Sheet)***

PI Name: Jeffrey Gander

PI Email: jg9br@virginia.edu

PI Phone # 434-243-4267

Name of Person Submitting this form: Rachel Simon

Contacts Email rmg5r@virgainia.edu

Contacts Phone # 434-243-7653

Protocol Title: Effect of Opiate Reduction on Clinical Outcomes and Hospital Cost in Neonates Undergoing Abdominal Surgery

Version Date: 11/27/2017

1. Will you be *Check at least one:*

a. ☒ Collecting data/specimens at UVA or personnel from UVA listed on this protocol are collecting data/specimens from site outside UVA

b. ☐ Receiving data/specimens from a person not listed on this protocol.

Submission may qualify for Non- human subject determination or Non-engaged Application.

c. ☐ Sending these data/specimens outside of UVA. *(Complete Appendix A)*

Submission may qualify for non-engaged application.

2. Specify how the specimens or data were initially collected

a. ☐ Data and/or specimens were collected under a different research protocol. The *research consent under which the original data/specimens were collected is provided with this submission.*

b. ☒ Data and/or Specimens were collected as part of clinical care and specimens are considered leftover from clinical care.

c. ☐ NA

3. **If you are receiving data/specimens from or sending data/specimens to an institution outside of UVA, do you confirm you have /will obtain a contract or a Material Transfer Agreement (MTA) prior to data/specimens being shared?**
☐ Yes ☐ No ☒ NA
If Yes, complete Appendix A.
Contract/MTA must be signed by official from Grants and Contracts or OSP.

4. **Do you confirm that no personnel from outside the UVa HIPAA covered entity will have access to identifiable health information?**
☒ Yes ☐ No
If you are collecting HIPAA identifiers AND health information this study does not meet exempt criteria.
If answered No, Privacy Board must require that the Health System HIPAA Authorization is signed by patients whose PHI is accessed even if not recorded.

5. **Provide a brief summary of the study**. The purpose of this study is to compare post-surgical outcomes in neonates under-going surgery before and after an opiate reduction intervention. We hypothesized that, due to decreased opiate administration, TPN days, return on bowel function, LOS, and total direct hospital costs will be lower in the reduced opiate group. A retrospective chart review (July 1, 2014- November 26,2017) will be done to evaluate these factors. Of note, the opiate reduction intervention was done as a clinical practice change at UVA in March of 2017.

6. **How do you plan to access the data/specimens or subjects?** Medical Records from UVA charts/medical records
Include specifics on sources of data (e.g. medical records from UVa charts/ medical records from non- UVa institution, registry outside of UVa etc) and or specimens (e.g. pathology, source outside of UVa. If subjects will be contacted provide specifics on how they will learn about the study.

7. **Describe the types of data/health information/human specimens will be obtained?** Data points to be collected are: gestational age at birth, birth weight, head circumference, birth weight, gender, type of operation, medical co-morbities, time to return of bowel function, time to full enteral feeds, days on TPN, days of mechanical ventilation, length of stay, procedure related complications, total hospital charges, and daily morphine equivalent dosing.

8. **Will the study team need to record any HIPPA identifier in order to gather information from more than one source?**
(Most commonly used would be name and medical record number)
☐ Yes ☒ No
If your answer to this question is yes- your protocol will NOT qualify for exempt approval if you are also collecting Health Information
IF YES, list HIPAA identifiers that will be needed:

9. **Do you confirm all study personnel will follow the requirements in the Privacy Plan (Appendix B)?**

☒ Yes ☐ No

Answer the questions below to verify compliance with DHHS (45CFR46) and FERPA (34 CFR Part 99) Regulations.

9A. Does this study involve:

☐Yes ☒ No	surveys or interviews given to minors?
☐Yes ☒ No	any procedures that may cause a subject either physical or psychological discomfort or are perceived as harassment above and beyond what the person would experience in daily life?
☐Yes ☒ No	deception?
☐Yes ☒ No	observation of minors if the investigator participates in the activities being observed unless there is a federal statute covering the activity?
☐Yes ☒ No	the study of a rare trait/disorder such that there is some risk of exposing the identity of sample donors or the research poses risk of community or cultural harm?
☐Yes ☒ No	Research that falls under the authority of the FDA (e.g. meets the FDA definitions below) **Human Subject**-an individual who is or becomes a participant in research, either as a recipient of the test article or as a control. A subject may be either a healthy human or a patient. C**linical Investigation** - any experiment that involves a test article and one or more human subjects and that either is subject to requirements for prior submission to the FDA, or is not subject to requirements for prior submission to the FDA under these sections of the Federal Food, Drug, and Cosmetic Act, but the results of which are intended to be submitted later to, or held for inspection by, the FDA as part of an application for a research or marketing permit. ***If data will be submitted to the FDA- answer this question YES***
☐Yes ☒ No	(a)research involving, after the delivery, the placenta, the dead fetus, macerated fetal material: or cells, tissue, or organs excised from a dead fetus, shall be conducted only in accord with any applicable Federal, State, or local laws and regulations regarding such activities? (b) if information associated with material described in paragraph (a) is recorded for research purposes in a manner that living individuals can be identified, directly or through identifiers linked to those individuals?
☐Yes ☒ No	Does the study involve an interaction or intervention with prisoners?
☐Yes ☒ No	Does the study involve collection of date of birth from students information governed by the federal FERPA regulations, such as information from Student Health, the Registrar's Office, the Office of Assessment and Studies, or the Student Information System (SIS)?

If you answer yes to any item above the protocol will NOT qualify for exempt approval.

9B. Does the study meet the following criteria?

Paragraph	☒Yes ☐ No	(1)Research involving the collection or study of *existing data*, documents, records, pathological specimens, or diagnostic specimens *Existing Data: means that all the data, documents, records, or specimens are in existence prior to IRB Review, therefore specimens obtained prospectively from*

		future discarded clinical samples do not qualify for exempt review.
	☒Yes ☐ No	(2)These sources (existing data, documents, records, pathological or diagnostic specimens) are publicly available **OR** the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects (*e.g. you answered NO to all HIPAA identifiers in Table C below*). *If both 1&2 checked: 45CFR46.101(b)(4)*
Paragraph 2	☐Yes ☒ No	(3)Research involving the use of: • educational tests, • survey procedures, • interview procedures • observation of public behavior **UNLESS** information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects **AND** that any disclosure of the human subject's responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subject's financial standing, employability or reputation. *45CFR46.101(b)(2)*
	☐Yes ☒ No	(4) OTHER: The project involves research conducted under another exemption criteria . *Copy and paste the applicable exemption criteria from the link here*

- *In order to qualify for exempt review the questions above must be answered either:*
  - *YES to # 1 AND # 2 and NO to # 3 OR*
  - *NO to # 1 and # 2 and YES to # 3 or # 4.*
- *If questions cannot be answered as above- Do not complete the rest of this form. Return to Protocol Builder and change the answer to the question regarding Exempt criteria to NO. Follow additional instructions in Protocol Builder to submit this protocol for expedited or full board review.*
- *IF 3 is checked above: CONSENT IS NOT REQUIRED FOR EXEMPT STUDIES HOWEVER USE OF VERBAL CONSENT OR OTHER METHODS CONSISTANT WITH WAIVER OF DOCUMENTATION OF CONSENT IS RECOMMENDED. IN ADDITION, IF THERE IS CONTACT SOMEONE OUTSIDE OF UVA HAS ACCESS TO PHI, THE PARTICIANT SHOULD BE REQUIRED TO SIGN THE UVA HEALTHSYSTEM HIPAA AUTHORIZATION.*

9b1. Does this study involve an interaction with a subject (survey, interview or observation where interaction is required? ☐ Yes ☒ No

IF YES, do you seek waiver of documentation of consent (verbal consent)? ☐ Yes ☐ No

IF YES, submit recruitment materials/ verbal consent script .

The following templates may be used:

- Email For Survey Studies conducted solely by email
- Letter Recruitment - For studies performed entirely by mail
- Verbal Consent Script Template - In Person
- Information sheet – information coversheet

9C. Answer the following questions to the best of your ability.

☐Yes ☒ No	Is the probability of the harm or discomfort anticipated in the proposed research greater than that encountered ordinarily in daily life or during the performance of

	routine physical or psychological examinations or tests?
☐Yes ☒ No	Is the magnitude of the harm or discomfort greater than that encountered ordinarily in daily life, or during the performance of routine physical or psychological examinations or tests?

If you answer yes to either question above the study will NOT qualify for exempt approval.

9D. Will you be banking blood/tissue? ☐ Yes ☒ No

If YES, answer the following two questions.

☐Yes ☐ No	Are the samples being collected for the sole purposes of this study?
☐Yes ☐ No	Are the specimens coded by a third party and stored in a facility that will not break the code, even upon the request of a family member or medical emergency or considered minimal risk?

If you answer yes to either question above the study will NOT qualify for exempt approval.

Answer the questions below to comply with HIPAA Regulations.(45CFR164)

10. Will you be collecting or using specimens OR collecting or using health information from patients or normal volunteers OR will someone from outside UVa have access to PHI via observation of healthcare?

☒ Yes *If yes, answer the question in 10A(1)*

☐ No ***If NO, HIPAA regulations do not apply. You are done. Do not answer any additional questions.***

10A(1) If this protocol has a sponsor, will the sponsor be coming to UVA to monitor this study OR observe healthcare providers administering care?

☐ Yes ☐ No ☒ NA

IF NO or NA- Skip to 10A(2)

IF YES:

- *Answer YES to the HIPAA identifiers that the sponsor/monitor/outside entity will see.*
- *Answer NO to the HIPAA identifiers that the sponsor/monitor/outside entity will NOT see.*

TABLE A: What the sponsor/monitor/outside entity sees?

☐Yes ☐ No	1. Name
☐Yes ☐ No	2. Postal address information, other than town or city, state, and zip code
☐Yes ☐ No	3. Telephone numbers
☐Yes ☐ No	4. Fax numbers
☐Yes ☐ No	5. Electronic mail addresses
☐Yes ☐ No	6. Social Security number
☐Yes ☐ No	7. Medical Record number
☐Yes ☐ No	8. Health plan beneficiary numbers
☐Yes ☐ No	9. Account numbers

☐Yes ☐ No	10. Certificate/license numbers
☐Yes ☐ No	11. Vehicle identifiers and serial numbers, including license plate numbers
☐Yes ☐ No	12. Device identifiers and serial numbers
☐Yes ☐ No	13. Web Universal Resource Locators (URLs)
☐Yes ☐ No	14. Internet Protocol (IP) address numbers
☐Yes ☐ No	15. Biometric identifiers, including finger and voice prints
☐Yes ☐ No	16. Full face photographic images and any comparable images

If you are doing a survey/interview/observation you are permitted to include any of the above identifiers as long as Health Information is NOT being recorded and the disclosure of the subject's responses would not place the subject at risk. NOTE: IF someone outside UVA observes patient care (has access to identifiers and PHI) then a UVA Health System HIPAA Authorization must be signed by the patients. Waiver of Documentation of Consent is encouraged in these cases.

10A(2). Will you record any of the following items regarding a potential subject, an enrolled subject, a subject's relative, household member or employer along with the data (which may include health information or be a specimen) or include the following items in a *linked file?

- *Answer YES to the HIPAA identifiers in the table below that you will record.*
- *Answer NO to the HIPAA identifiers in the table below that you will NOT record.*
- *Note: *linked file- means that your subject code (e.g. subject #1) are "linked" to identifier(s). You may have this link in a separate list, but if you are keeping information anywhere that connects subject codes to Identifiers, (e.g. subject #1 is John Doe or medical record # 123456) then you are maintaining a linked file.*

TABLE B: Identifiers per HIPAA under 164.514(b)(2)(i) and (ii)

☐Yes ☒ No	1. Name
☐Yes ☒ No	2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of the zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people and (2) The initial 3 digits of a zip code for all such geographic units containing 20,000 is changed to 000.
☐Yes ☒ No	3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older. *[This means you may record the year but not record the month or day of any date related to the subject if the subject is under the age of 89. In addition if the subject is over the age of 89 you may not record their age and you may not record the month, day or year of any date related to the subject]*
☐Yes ☒ No	4. Telephone numbers
☐Yes ☒ No	5. Fax numbers
☐Yes ☒ No	6. Electronic mail addresses
☐Yes ☒ No	7. Social Security number
☐Yes ☒ No	8. Medical Record number
☐Yes ☒ No	9. Health plan beneficiary numbers

☐Yes ☒ No	10. Account numbers
☐Yes ☒ No	11. Certificate/license numbers
☐Yes ☒ No	12. Vehicle identifiers and serial numbers, including license plate numbers
☐Yes ☒ No	13. Device identifiers and serial numbers
☐Yes ☒ No	14. Web Universal Resource Locators (URLs)
☐Yes ☒ No	15. Internet Protocol (IP) address numbers
☐Yes ☒ No	16. Biometric identifiers, including finger and voice prints
☐Yes ☒ No	17. Full face photographic images and any comparable images
☐Yes ☒ No	18. Any other unique identifying number, characteristic, code that is derived from or related to information about the individual (*e.g. initials, last 4 digits of Social Security #, mother's maiden name, first 3 letters of last name.)*
☐Yes ☒ No	19. Any other information that could be used alone or in combination with other information to identify an individual. (*e.g. rare disease, study team or company has access to the health information and a HIPAA identifier or the key to the code* .)

- *If you answered yes to any item above, except # 2 or 3, the study MAY NOT qualify for exempt approval.*
- *If you are doing a survey/interview/observation you are permitted to include any of the above identifiers as long as Personal Health Information (PHI) is NOT being recorded and the disclosure of the subject's responses would not place the subject at risk.*

10B. Answer the following question to the best of your ability.

☐Yes ☒ No	Do you have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information? *If you have answered YES to any item, except # 2 or 3 in TABLE B, then the response for this question must be YES.*

10B(1). If you checked YES to any of the items in TABLE B do you plan to disclose the information outside of UVA with any of the identifiers from Table B?

☐ Yes ☐ No ☒ NA

10B(2). If 10B(1) is YES, which items checked above will be disclosed outside of UVa? NA

- ***If you answered NO to all items in10A and 10B, the data meets the criteria of de-identified under HIPAA.***
- ***You are done-you do not need to answer any additional questions.***
- *If you answered YES to any of the items 10A or 10B please answer questions 10C and 10D.*

10C. Will you record any of the following items regarding a potential subject, an enrolled subject, a subject's relative, household member or employer along with the data (which may include health information or be a specimen) or include the following items in a *linked file?

- *Answer YES to the HIPAA identifiers in the table below that you will record.*
- *Answer NO to the HIPAA identifiers in the table below that you will NOT record.*
- *Note: *linked file- means that your subject code (e.g. subject #1) are "linked" to identifier(s). You may have this link in a separate list, but if you are keeping information anywhere that connects subject codes to Identifiers, (e.g. subject #1 is John Doe or medical record # 123456) then you are maintaining a linked file.*

TABLE C: Limited Data Set criteria per HIPAA under 164.514(e)

☐Yes ☐ No	1. Name
☐Yes ☐ No	2. Postal address information, other than town or city, state, and zip code
☐Yes ☐ No	3. Telephone numbers
☐Yes ☐ No	4. Fax numbers
☐Yes ☐ No	5. Electronic mail addresses
☐Yes ☐ No	6. Social Security number
☐Yes ☐ No	7. Medical Record number
☐Yes ☐ No	8. Health plan beneficiary numbers
☐Yes ☐ No	9. Account numbers
☐Yes ☐ No	10. Certificate/license numbers
☐Yes ☐ No	11. Vehicle identifiers and serial numbers, including license plate numbers
☐Yes ☐ No	12. Device identifiers and serial numbers
☐Yes ☐ No	13. Web Universal Resource Locators (URLs)
☐Yes ☐ No	14. Internet Protocol (IP) address numbers
☐Yes ☐ No	15. Biometric identifiers, including finger and voice prints
☐Yes ☐ No	16. Full face photographic images and any comparable images

10D. Please answer the following question to the best of your ability.

☐Yes ☐ No	Will this information be disclosed for purposes other than research, public health, or health care operations of the University of Virginia Health System?

- ***If you answered NO to all items in 10C and 10D your data meets the criteria of a Limited Data Set. You are done.***
- ***If you answered YES to any item in 10C or 10D your data is considered "Identified"*** *and does not qualify for exempt approval. Return to Protocol Builder and change the answer to the question regarding Exempt criteria to NO. Follow additional instructions in Protocol Builder to submit this protocol for expedited or full board review.*

Appendix A: Information (Data/ Specimens) from Outside Institution

INSTRUCTIONS:
You will need to submit an IRB approval or documentation from the outside institution documenting that they approve of this study being done at their site and info being shared with UVa.
In order to obtain information from other sites in the future, you will be required to submit a modification of this protocol to the IRB-HSR.

1. **List the names of outside institutions that will be supplying data and/or specimens for this study.**
   Answer/Response:

2. **Describe the type of information you will receive from each site.**
   Answer/Response:

3. **Does the outside institution have an IRB?**
   Answer/Response:

   IF NO, list the names of the individuals who will be supplying the data and/or specimens.

   INSTRUCTIONS: You will be required to submit a signed Unaffiliated Investigator Agreement for each person listed.

   Answer/Response:

Appendix B: Privacy Plan

Privacy Plan

The following procedures must be followed.

- The data will be secured per the Data Security Plan of this protocol.
- Only investigators for this study and clinicians caring for the patient will have access to data. They will each use a unique login ID and password that will keep confidential. The password should meet or exceed the standards described on the Information Technology Services (ITS) webpage about *The Importance of Choosing Strong Passwords.*
- Each investigator will sign the University's Electronic Access Agreement forward the signed agreement to the appropriate department as instructed on the form.

  If you currently have access to clinical data it is likely that you have already signed this form. You are not required to sign it again.
- UVa University Data Protection Standards will be followed.
- If identifiable data is transferred to any other location such as a desktop, laptop, memory stick, CD etc. the researcher must follow the University's Highly Sensitive Data Protection Standard for Individual-Use Electronic Devices or Media Additional requirements may be found in the University's Security of Network-Connected Devices Standard. If identifiable data is taken away from the UVa Health System, Medical Center Policy # 0218 will be followed.
- Data will be securely removed from the server/drive, additional computer(s), and electronic media according to the University's Electronic Data Removal Standard.
- Data will be encrypted or removed if the electronic device is sent outside of UVa for repair according to the University's Electronic Data Removal Standard .
- If PHI will be faxed, researchers will follow the Health System Policy # 0194.
- If PHI will be emailed, researchers will follow the Health System Policy # 0193 and University Data Protection Standards (UDPS 3.0).
- Data may not be analyzed for any other study without additional IRB approval.
- If you are using patient information you must follow Health System Policy # 0021.
- Both data on paper and stored electronically will follow the University's Record Management policy and the Commonwealth statute regarding the Destruction of Public Records.

If you have a question or concerns about the required security standards contact InfoSec at it-security@virginia.edu

Summary of Requirements to Comply with UVa Health System, Medical Center and University Policies and Guidance as noted above:

Highly Sensitive Data is:
-personal information that can lead to identity theft if exposed or
-data that reveals an individual's health condition and/or history of health services use.
Protected Data (PHI) a type of Highly Sensitive Data, is data combined with a HIPAA identifier
Identifiable Data under HIPAA regulations is considered to be *Highly Sensitive Data at UVa.*
A **Limited Data Set** (LDS) under HIPAA regulations is considered to be *Moderately Sensitive Data* at UVa. The only HIPAA identifiers associated with data: dates and or postal address information limited to town or city, state, and zip code.

Highly Sensitive Data (Identifiable Health Info per HIPAA)	**Moderately Sensitive Data (Limited Data Set and De-identified data per HIPAA)**
General Issues	*General Issues*
Discussions in private Do not share with those not on the study team or those who do not have a need to know.	Do not share with those not on the study team or those who do not have a need to know.
Password protect	Password protect
Physically secure (lock) hard copies at all times if not directly supervised. If not supervised hard copies must have double protection (e.g. lock on room OR cabinet AND in building requiring swipe card for entrance).	Physically secure (lock) hard copies at all times if not directly supervised.
For electronic documents turn off File Sharing; turn on firewalls; use up to date antivirus and antispyware; delete data securely.	For electronic documents turn off File Sharing; turn on firewalls; use up to date antivirus and antispyware; delete data securely.
Encrypt See Encryption Solutions Guidance *Files on Health System Network drives are automatically encrypted. If not stored there it is study teams responsibility to make sure data are encrypted.*	
If device sent out for service or repair, encrypt or remove data AND contract for repair using a UVa Purchase order.	If device sent out for service or repair, encrypt or remove data AND contract for repair using a UVa Purchase order.
Store files on a network drive specifically designated for storing this type of data, e.g. high-level security server/drives managed by Information Technology Services or the "F" and "O" managed by Heath Systems Computing Services. You may access it via a shortcut icon on your desktop, but you are not allowed to take it off line to a local drive such as the desktop of your computer (e.g. C drive) or to an individual Use Device*. May access via VPN	
Do not share with sponsor or other outside group before consent is obtained or the IRB has granted appropriate approvals and contract/ MTA is in place	Do not share with sponsor or other outside group before consent is obtained or the IRB has granted appropriate approvals and contract/ MTA is in place
If collected without consent/ HIPAA authorization will NOT be allowed to leave UVa HIPAA covered entity unless disclosure is approved by the IRB and the disclosure is tracked in EPIC	If collected without consent/ HIPAA authorization will NOT be allowed to leave UVa HIPAA covered entity unless disclosure is approved by the IRB and an MTA is in place prior to sharing of data

Highly Sensitive Data **(Identifiable Health Info per HIPAA)**	**Moderately Sensitive Data** **(Limited Data Set and De-identified data per HIPAA)**
Electronic Data Collection & Sharing	*Electronic Data Collection & Sharing*
(e.g. smart phone app, electronic consent using tablet etc.) MUST consult with InfoSec or Health System Web Development Office: 434-243-6702 ▪ University Side: IT-Security@virginia.edu ▪ Health System: Web Development Center:	
Individual-Use Device	*Individual-Use Device*
Do not save to individual-use device* without written approval of your Department AND VP or Dean. If approval obtained, data must be password protected and encrypted.	
Do not save an email attachment containing HSD to an individual use device (e.g. smart phone)	
E Mail	*E Mail*
Do not share via email with Outlook Web/ or forward email using other email vendors like Gmail/ Yahoo	
Do not send via email on smart phone unless phone is set up by Health System	
Email may include name, medical record number or Social Security number only if sending email to or from a person with * HS in their email address. *NOTE: VPR & IRB staff do not meet this criteria!*	In addition to sharing LDS, may include initials if persons sending and receiving email work within the UVa HIPAA covered entity.**
FAX	*FAX*
Verify FAX number before faxing	Verify FAX number before faxing
Use Fax Cover Sheet with Confidentiality Statement	Use Fax Cover Sheet with Confidentiality Statement
Verify receiving fax machine is in a restricted access area	Verify receiving fax machine is in a restricted access area
Verify intended recipient is clearly indicated	Verify intended recipient is clearly indicated
Recipient is alerted to the pending transmission and is available to pick it up immediately	Recipient is alerted to the pending transmission and is available to pick it up immediately

Highly Sensitive Data (Identifiable Health Info per HIPAA)	Moderately Sensitive Data (Limited Data Set and De-identified data per HIPAA)
Electronic Data Collection & Sharing	*Electronic Data Collection & Sharing*
(e.g. smart phone app, electronic consent using tablet etc.) MUST consult with InfoSec or Health System Web Development Office: 434-243-6702 University Side: IT-Security@virginia.edu Health System: Web Development Center: Contract must include required security measures.	
May be stored in UVA's Qualtrics portal for Highly Sensitive Data (HSD) May NOT be stored in places like UVaBox, UVaCollab or QuestionPro May also NOT be stored in non-UVa licensed cloud providers, such as Dropbox, Google Drive, SkyDrive, Survey Monkey, etc.	May be stored in places like UVaBox, UVaCollab, UVA's Qualtrics portal for Moderately Sensitive Data May NOT be stored in non-UVa licensed cloud providers, such as Dropbox, Google Drive, SkyDrive, Survey Monkey, etc.

** Individual Use Device – examples include smart phone, CD, flash (thumb) drive, laptop, C drive of your computer,*
***The UVa HIPAA covered entity includes the UVa VP Office of Research, the Health System, School of Medicine, School of Nursing, Nutrition Services (Morrison's), the Sheila C. Johnson Center, the Exercise and Sports Injury Laboratory, the Exercise Physiology Laboratory and the UVA Center for Survey Research.*

Appendix C:

For IRB-HSR Use Only- Exempt Determination

IRB-HSR #/UVA Study Tracking#: 20324
Protocol Title: Effect of Opiate Reduction on Clinical Outcomes and Hospital Cost in Neonates Undergoing Abdominal Surgery

The IRB-HSR confirms that this project meets the criteria of research which is exempt from federal regulations under 45CFR46.101 (b)(4).

The study includes only collection of de-identified health information therefore HIPAA regulations do not apply.

You are required to protect the data according to the enclosed Privacy Plan and the Data Security Plan.
If you need to modify the procedures in this project you must submit an email to IRBHSR@virginia.edu describing the changes. The IRB-HSR will determine if the project continues to meet the criteria for exempt research.
Closure: When this study is complete there is no need to submit a Closure Form. Any Closure Form submitted will be returned to you unprocessed by the IRB.
For additional information regarding educational resources for research see http://www.virginia.edu/vpr/irb/hsr/education.html

Signed Joanna Faulconer **Date** November 29, 2017
IRB-HSR Staff Member

Data Use Agreement

IRB-HSR #/UVA Study Tracking #:

INSTRUCTIONS: Data being used in this protocol meets the criteria of a Limited Data Set. To comply with HIPAA regulations the principal investigator of this protocol must sign this memo regarding Limited Data Sets. This memo must be filed with your regulatory files and kept for 6 years from the date of protocol closure with the IRB-HSR.

This memorandum is designed to permit you to use and disclose a "Limited Data Set" of patients' health information for UVA in compliance with the HIPAA Privacy Rule, 45 CFR Parts 160 and 164, subparts A and E.1.

1. Except as otherwise specified in this memorandum, you may use and disclose the Limited Data Set for research purposes only as described in the Research Protocol. You represent that the Limited Data Set is the minimum amount of data necessary for the conduct of the Research Protocol.

2. You agree not to use or disclose the Limited Data Set for research purposes other than as permitted by this Agreement or as otherwise required by law.

3. You agree to use appropriate safeguards as described in your protocol to prevent the use or disclosure of the Limited Data Set other than as provided for by this Agreement.

4. You agree to promptly report to the IRB for Health Sciences Research Office any use or disclosure of the Limited Data Set not described in your protocol or in this memo of which you become aware.

5. You agree to contact the IRB for Health Sciences Research Office prior to providing information from the Limited Data Set to any person or entity outside the University, so that the recipient can be required to agree to the same restrictions and conditions in this memorandum.

6. You agree not to attempt to identify the patients to whom the information contained in the Limited Data Set pertains in order to contact those individuals for purposes of research.

_____ _____

Principal Investigator Date

DATA SECURITY PLAN

Version Date: **11/28/2017**
IRB HSR Submission # **12351**
IRB-HSR # 20324 Will be completed by the IRB-HSR staff.

General Information

You should consult with ISPRO during the development phase of this protocol if your protocol will involve highly technical issues such as the creation of a website to collect data, software application development, the use of a smart phone app, or if you plan to store identifiable data ONTO an individual use device such as a tablet/laptop/camera. Otherwise submit the protocol and this Data Security Plan to the IRB-HSR for pre-review. The IRB-HSR will notify the study team and ISPRO if ISPRO approval is required. .

ISPRO CONTACT INFORMATION:
UVa Office of Information Security, Policy & Records Office (ISPRO)
www.virginia.edu/ispro
Email: IT-Security@Virginia.edu

Glossary of terms located at end of document.

Completion Instructions

1. Read questions carefully and answer questions as indicated.
2. For questions, contact ISPRO IT-Security@Virginia.edu
3. Use the following instructions to provide the server name. **INSTRUCTIONS:**
   - You may locate the server/drive name and path by taking the following steps :
     - In Windows under computer, right click on the Drive icon (e.g. F). Then click on Properties. The server/drive name and path will appear at the very top of the box.
     - If you need additional assistance contact your department computer support or system administrator for assistance.

Submission Instructions

The IRB-HSR will submit the protocol to ISPRO after the pre-review is completed if their review is required.

DATA COLLECTION

1A. Will any HIPAA identifiers be collected or received by the UVa study team?

INSTRUCTIONS:

- Answer YES if you are collecting, recording or receiving any of these items for a potential subject, an enrolled subject, a subject's relative, household member or employer.
- Answer YES even if you are recording any item below temporarily while the information is being collected.
- Keep in mind that the information below includes data collected via photographs, video, audiotapes, and systems like IVRS (Interactive Voice Response System)
- If you answer NO to all items it means you would never be able to go back and obtain any additional information about an individual.

YES	NO	HIPAA Identifier
☐	☒	1. Name
☐	☒	2. Postal address information, other than town or city, state, and zip code
☐	☒	3. Telephone numbers
☐	☒	4. Fax numbers
☐	☒	5. Electronic mail addresses
☐	☒	6. Social Security number- *Must be checked if you are collecting SS# for compensation.*
☐	☒	7. Medical Record number
☐	☒	8. Health plan beneficiary numbers
☐	☒	9. Account numbers (e.g. bank numbers, credit card numbers, hospital bill account number)
☐	☒	10. Certificate/license numbers (e.g. passport number, driver's license number, medical board license number)
☐	☒	11. Vehicle identifiers and serial numbers, including license plate numbers
☐	☒	12. Device identifiers and serial numbers
☐	☒	13. Web Universal Resource Locators (URLs)
☐	☒	14. Internet Protocol (IP) address numbers
☐	☒	15. Biometric identifiers, including finger and voice prints
☐	☒	16. Full face photographic images and any comparable images

INSTRUCTIONS:

If you checked NO to all HIPAA Identifiers above your data is considered to be MODERATELY SENSITIVE.

Follow requirements for handling moderately sensitive data in the Privacy Plan of the protocol.

Do not answer any additional questions. No review by ISPRO is required.

If you checked YES to any item above, continue to question 1B.

1B. Check ALL applicable items below to describe HOW DATA will be COLLECTED:

►IMPORTANT: If you check any of the items 1B(1) through 1B(3) below and you will be collecting HIPAA identifiers with the information, the protocol may require review and approval by ISPRO. The IRB-HSR office staff will notify ISPRO if their review is required.

1B(1). ☐

Collection of data ONTO* an individual-use device (examples include desktop computer, smart phone app, flash (thumb) drive, external hard drive, tablet, laptop, CD, C drive of your computer, camera, video or audio recorder)

*ONTO means the data will reside on OR will be stored on the device even if temporarily.

Do not check this box if the device will simply be used to access a server.

IF CHECKED:

Describe the individual use device: (e.g., smart phone) _____

LIST all HIPAA identifiers to be collected: _____

AND COMPLETE APPENDIX 1B(1) below.

1B(2.) ☐

Collection of data via web-based format or cloud storage (e.g., UVaBox, UVa-Collab or other cloud service OR online consent, online surveys)

DO NOT check if data will be collected directly to a server/drive managed by the sponsor or CRO (use item 1B(5) below if server managed by sponsor or CRO).

IF CHECKED:

List the web address (URL): _____

LIST all HIPAA identifiers to be collected: _____

AND COMPLETE APPENDIX 1B(2) below.

1B(3). ☐

Collection of data directly to a server at UVa NOT listed under 1B(4) below.

IF CHECKED:

List the name of the server (e.g. name.virginia.edu\project name): _____

LIST all HIPAA identifiers to be collected: _____

AND COMPLETE APPENDIX 1B(3) below.

►IMPORTANT: If you check any of the items 1B(1) through 1B(3) above and you will be collecting HIPAA identifiers with the information, the protocol may require review and approval by ISPRO. The IRB-HSR office staff will notify ISPRO if their review is required.

1B(4). ☐

Collection of data directly to one or more of the UVa servers checked below.

IF CHECKED,

LIST all HIPAA identifiers to be collected onto this device: _____

AND COMPLETE APPENDIX 1B(4) below

- ☐ domatlas.eservices.virginia.edu
- ☐ dom-titan.eservices.virginia.edu
- ☐ Elson1.studenthealth.virginia.edu
- ☐ EPIC
- ☐ es3.eservices.virginia.edu
- ☐ gcrcserver.itc.virginia.edu
- ☐ \\HSCS-ss7
- ☐ \\HSCS-ss8
- ☐ \\HSCS-ss9

☐ \\HSCS-ss10
☐ \\HSCS-ss11
☐ \\HSCS-ss12
☐ \\HSCS-ss13
☐ \\hscs-share1\
☐ \\hscs-share2\
☐ \\hscs-share3\
☐ hstsdatalab.hscs.virginia.edu
☐ hstsdsmpogapp.hscs.virginia.edu
☐ Ivy Secure Computing Platform/ Ivy Secure Cloud/Ivy Cloud
☐ musicvpn01.med.virginia.edu
☐ Oncore (oncore.med.virginia.edu)
☐ School of Nursing SECURE NETf
☐ Redcap-int.hscs.virginia.edu
☐ \\radshare\
☐ upgusers.hscs.virginia.edu

1B(5). ☐
Collection of data directly to a server/drive managed by the sponsor or CRO.
Data must be sent and stored in an encrypted fashion (e.g. must be shared and stored via Secure FX, Secure FTP, HTTPS, PGP) and the server/drive is configured to store data regulated by HIPAA.

IF CHECKED:

List the name of the server (e.g. remote.sponsor.com\project name): _____
LIST all HIPAA identifiers to be collected onto this server: _____
AND COMPLETE APPENDIX 1B(5) below

1B(6). ☐ Paper -

IF CHECKED:

List ALL the HIPAA identifiers to be stored in paper file(s): _____
Remember: Initials are considered a HIPAA identifier!

►If health information with HIPAA identifiers are stored in a paper file, where will the paper files be housed?

☐ Signed consent forms or documentation regarding obtaining verbal consent will be stored in a *secure area with limited access.*
☐ Case report forms will be stored in a *secure area with limited access.*
☐ Questionnaires/surveys will be stored in a *secure area with limited access.*
☐ Other - *Specify* _____

NOTE: "*in a secure area with limited access*" means access to data is limited to study personnel only and there must be two forms of security. Example: 1) in a locked office in a building with swipe locks when unattended or 2) in a locked file cabinet in a locked room when unattended or 3) study personnel present in room at all times located in a building with swipe locks or a room with a lock,

DATA STORAGE

1C. Will any data be <u>stored electronically (e.g. during data analysis and/or beyond)</u> ?

Yes ☐ No ☐ *IF NO, skip to item 1C(1)b.*

1C(1)►IF YES, will it include storage of any health information or other sensitive data?

Yes ☐ No ☐

1C(1)a If YES, check the HIPAA identifiers in the table below that will be kept with highly sensitive data in the same location (e.g. on the same electronic drive,server or file).

YES	NO	HIPAA Identifier
☐	☐	1. Name
☐	☐	2. Postal address information, other than town or city, state, and zip code (e.g. street name or GPS)
☐	☐	3. Telephone numbers
☐	☐	4. Fax numbers
☐	☐	5. Electronic mail addresses
☐	☐	6. Social Security number- *Must be checked if you are collecting SS# for compensation.*
☐	☐	7. Medical Record number
☐	☐	8. Health plan beneficiary numbers
☐	☐	9. Account numbers (e.g. bank numbers, credit card numbers, hospital bill account number)
☐	☐	10. Certificate/license numbers (e.g. passport number, driver's license number, medical board license number)
☐	☐	11. Vehicle identifiers and serial numbers, including license plate numbers
☐	☐	12. Device identifiers and serial numbers
☐	☐	13. Web Universal Resource Locators (URLs)
☐	☐	14. Internet Protocol (IP) address numbers
☐	☐	15. Biometric identifiers, including finger and voice prints
☐	☐	16. Full face photographic images and any comparable images

INSTRUCTIONS: <u>If you checked YES</u> to any HIPAA Identifier above your data is considered to be HIGHLY SENSITIVE.

Follow requirements for handling Highly Sensitive data in the Privacy Plan of the protocol.

1C(1)b. Will you store any of the following HIPAA identifiers electronically in a different location from the data?

YES	NO	HIPAA Identifier
☐	☐	Social Security number- *Must be checked if you are collecting SSN for compensation.*
☐	☐	Account numbers (e.g. bank numbers, credit card numbers, hospital bill account number)
☐	☐	Certificate/license numbers (e.g. passport number, driver's license number, medical board license number)

IF YOU CHECKED YES to any Identifier above:
List the name of the server (e.g. name.virginia.edu\project name):_____

INSTRUCTIONS: If you checked YES to any HIPAA Identifier above your data is considered to be HIGHLY SENSITIVE. Follow requirements for handling Highly Sensitive data in the Privacy Plan of the protocol.

1C(2). WHERE will the data be stored long term (e.g. during data analysis and beyond) by you (UVa) and/or the sponsor?

☐ Data will be stored in the same location to which it was collected or transferred as noted in 1B *(Skip to Transferring Data)*

You may check 1C(2) above and also add a new place where data will be stored that was not a location where it was collected. For example, you may have checked 1B(2) for collection of data, and plan to store it both in same location as 1B(2) as well as store on HSCS server. So you could check 1C(2) above and just fill out 1C(1)d below.

If you did not answer the option above, check an applicable option below.

1C(2)a. ☐
*ONTO** an individual-use device (*examples include desktop computer, smart phone app, flash (thumb) drive, external hard drive, tablet, laptop, CD, C drive of your computer)*
**ONTO means the data will reside or be stored on the device even if temporarily. Do not check this box if the device will simply be used to access a server.*
IF CHECKED:
Describe the individual use device: (e.g., smart phone)
*LIST all HIPAA identifiers to be stored:*_____
AND COMPLETE APPENDIX 1C(2)a below
ISPRO approval mayl be required. The IRB-HSR staff will send the protocol and Data Security Plan to ISPRO after pre-review is completed if ISPRO approval is required.

1C(2)b. ☐
Web-based or cloud storage (e.g., UVaBox, UVa-Collab or other cloud service)

IF CHECKED:

*LIST the web address (URL):*_____

*LIST all HIPAA identifiers to be stored:*_____

AND COMPLETE APPENDIX 1C (2)b below.

ISPRO approval may be required. The IRB-HSR staff will send the protocol and Data Security Plan to ISPRO after pre-review is completed if ISPRO approval is required.

1C (2)c. ☐

On a server at UVa NOT listed under 1C(2)d below.

IF CHECKED:

List the name of the server/drive (e.g. name.virginia.edu\project name): _____

*LIST all HIPAA identifiers to be stored:*_____

AND COMPLETE APPENDIX 1C2(c) below.

ISPRO approval may be required. The IRB-HSR staff will send the protocol and Data Security Plan to ISPRO after pre-review is completed if ISPRO approval is required.

1C(2)d. ☐

Directly to one or more of the UVa servers listed below.

IF CHECKED:

*LIST all HIPAA identifiers to be stored:*_____

AND COMPLETE APPENDIX 1C(2)d.

☐ domatlas.eservices.virginia.edu
☐ dom-titan.eservices.virginia.edu
☐ Elson1.studenthealth.virginia.edu
☐ EPIC
☐ es3.eservices.virginia.edu
☐ gcrcserver.itc.virginia.edu
☐ \\HSCS-ss7
☐ \\HSCS-ss8
☐ \\HSCS-ss9
☐ \\HSCS-ss10
☐ \\HSCS-ss11
☐ \\HSCS-ss12
☐ \\HSCS-ss13
☐ \\hscs-share1\
☐ \\hscs-share2\
☐ \\hscs-share3\
☐ hstsdatalab.hscs.virginia.edu
☐ hstsdsmpogapp.hscs.virginia.edu
☐ Ivy Secure Computing Platform/ Ivy Secure Cloud/Ivy Cloud
☐ musicvpn01.med.virginia.edu
☐ Oncore (oncore.med.virginia.edu)
☐ School of Nursing SECURE NETf
☐ Redcap-int.hscs.virginia.edu
☐ \\radshare\
☐ upgusers.hscs.virginia.edu

1C(2)e. ☐

A server/drive managed by the sponsor or CRO. The data must be sent and stored in an encrypted fashion (e.g. must be shared and stored via Secure FX, Secure FTP, HTTPS, PGP) onto a server/drive that is configured to store data regulated by HIPAA.

IF CHECKED:

List the name of the server (e.g. remote.sponsor.com\project name): _____

LIST all HIPAA identifiers to be stored: _____

AND COMPLETE APPENDIX 1C(2)e.

DATA TRANSFER

1E(1) Will you be sharing/transferring data outside of UVa? Yes ☐ No ☐
If YES, Will any of the following HIPAA identifiers be shared/transported with the data outside of UVa?

Limited Data Set criteria per HIPAA under 164.514(e)

☐Yes ☐ No	1. Name
☐Yes ☐ No	2. Postal address information, other than town or city, state, and zip code
☐Yes ☐ No	3. Telephone numbers
☐Yes ☐ No	4. Fax numbers
☐Yes ☐ No	5. Electronic mail addresses
☐Yes ☐ No	6. Social Security number
☐Yes ☐ No	7. Medical Record number
☐Yes ☐ No	8. Health plan beneficiary numbers
☐Yes ☐ No	9. Account numbers
☐Yes ☐ No	10. Certificate/license numbers
☐Yes ☐ No	11. Vehicle identifiers and serial numbers, including license plate numbers
☐Yes ☐ No	12. Device identifiers and serial numbers
☐Yes ☐ No	13. Web Universal Resource Locators (URLs)
☐Yes ☐ No	14. Internet Protocol (IP) address numbers
☐Yes ☐ No	15. Biometric identifiers, including finger and voice prints
☐Yes ☐ No	16. Full face photographic images and any comparable images

1E(2).If you checked YES to any item above have you obtained written HIPAA authorization to share the data with the specific group outside of UVa?

Yes ☐ No ☐

If NO, NOTE: No data collected without consent/HIPAA authorization or collected under verbal consent/HIPAA authorization may be shared outside of UVa with any of the HIPAA identifiers checked above unless the IRB has approved the disclosure and tracking the disclosure in EPIC is performed by the study team.

1E(3). How will the data be shared/transported?

☐ **Paper forms**

If shipped outside of UVa must be shipped with tracking (FedEx, UPS, certified mail etc.)
Messenger mail not allowed if you have answered YES to any item above

☐ **Email:**

Not allowed if you have answered YES to any item above unless *the data will only be sent to and from an individual with a *HS in their email address*

☐ **Secure Email:**

Not allowed if you have answered YES to any item above UNLESS you use the HSC Mail System and follow the steps listed at: https://www.hsts.virginia.edu/services/it-security/how-tos/encrypted-email

☐ **FAX:**

Not allowed unless receiving fax machine is in a restricted-access location, the intended recipient is clearly indicated, and that recipient has been alerted to the pending transmission and is available to pick it up immediately. Also verify FAX numbers before faxing and use FAX cover sheet with a confidentiality statement.

☐ **Devices such as flash-drive/ CD etc.:**

Not allowed if you have answered YES to any item in 1E(1) unless you written approval from a VP/ Dean. The request for their written approval should be obtained using the Highly Sensitive Data Storage Request Form. You may also contact the UVa Office of Information, Security, Policy and Records Management at IT-Security@Virginia.edu for assistance in completing this form.

☐ **Web Based Data Entry (e.g. website, database, registry): NOT Encrypted and Password Protected;**

Not allowed if you have answered YES to any item 1E(1).

☐ **Web Based Data Entry (e.g. website, database, registry): Encrypted and Password Protected;**

If checked, do you confirm that you have verified with host site that the data will be sent and stored in an encrypted fashion (e.g. via Secure FX, Secure FTP, HTTPS, PGP)?

Yes ☐ No ☐

IF CHECKED COMPLETE DATA SECURITY PLAN APPENDIX 1B(5) if not already completed.

INSTRUCTIONS: Do not complete the questions below if the only data being shared/transported are being sent with specimens. See Specimens Section

1E(4) If sharing data with anyone outside of UVa do you confirm that you will obtain a contract/ material transfer agreement with them via the School of Medicine Grants and Contracts Office or the Office of Sponsored Programs (OSP) ospnoa@virginia.edu**?**

Yes ☐ No ☐

1E(5) Will any data be sent outside of UVa to any person at another institution other than the sponsor or the FDA (e.g. researcher outside of UVa)?

Yes ☐ No ☐

INSTRUCTIONS:
If NO, skip questions 1E(5))a-d below

1E(5)a. What will be shared?

*List the data to be shared, including any HIPAA identifiers:*_____

1E(5)b. Who will the data be shared with?

_____

1E(5)c. What will they do with the data?

_____

1E(5)d. Will information be sent back to UVa? Yes ☐ No ☐

If yes, *LIST the data to be sent back, including any HIPAA identifiers:*_____

If yes, *how it will sent back (see the list under 1E(3) for possible methods)*?

_____

END OF FORM- COMPLETE THE APPENDIX SECTIONS THAT FOLLOW ONLY IF APPLICABLE.

Data Security Plan: APPENDIX 1B(1)

1B(1). Collection of data *ONTO** an individual-use device (*examples include desktop computer, smart phone app, flash (thumb) drive, external hard drive, tablet, laptop, CD, C drive of your computer, camera, audio or video recorder)*

- What kind of device is it (*examples include desktop computer, smart phone app, flash (thumb) drive, external hard drive, tablet, laptop, CD, C drive of your computer, camera, audio or video recorder)* _____

- Who manages / supports the device (e.g., Health Systems Computing Services (HS/CS), local computer support partner (LSP), self)? _____

  INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

- Will the data be transferred elsewhere? Yes ☐ No ☐

  - INSTRUCTIONS:
  - *If NO, you must complete Appendix 1C(2)a below and if you will store health information with any of the identifiers check in the table 1A on page 2 you must also complete and have signed a* ***Highly Sensitive Data Storage Request form available at:*** www.virginia.edu/informationsecurity/highlysensitivedata/approvalform.doc
  - *If YES, answer the following four questions*

  1. Will the data be transferred in an encrypted secure manner such as the use of SFTP or HTTPS? Yes ☐ No ☐
     - Describe transfer method: _____

  2. How long will the data remain on the individual-use device before being transferred? _____

  3. Please provide the location the data are transferred to:_____

  4. After the information is transferred elsewhere will you securely delete all data from the website/server? Yes ☐ No ☐

  INSTRUCTIONS: For computers not using Windows 8 or newer, download and use the Secure Delete Program from ITS. If using Windows 8 or newer, click on Secure Delete when deleting a file. For Macintosh computers, select "Secure Empty Trash" from the Finder menu.

- Will anyone other than study team members have access to data on the device? Yes ☐ No ☐ If yes, describe: _____

- Are any backups made of the information on the device? Yes ☐ No ☐
  - If yes, explain how backups are made and where they are stored: _____

- Does the owner of the device (e.g. phone service provider/ app developer) have any rights to use or access data either individually or in aggregate? Yes ☐ No ☐

Data Security Plan: APPENDIX 1B(1) continued

- Are you doing any audio or videotaping (recording)? Yes ☐ No ☐ N/A ☐
    - If yes, have you completed the Taping/Photography section in the protocol? Yes ☐ No ☐ N/A ☐

- If you are using an individual use device such as a camera or video recorder do you confirm the photos will not include the full face. Yes ☐ No ☐ N/A ☐

- If you are using a video or audio recorder, do you confirm the data will not include HIPAA identifiers? Yes ☐ No ☐ N/A ☐

END OF APPENDIX 1B(1)

Data Security Plan: APPENDIX 1B(2)

1B(2.) Collection of data via web-based or cloud storage (e.g. UVaCollab, UVaBox, or online consent, online surveys or any cloud service)

- Provide the name of the website or cloud storage (e.g.,URL): _____

NOTE: No research data of any kind may be stored in a non-UVa licensed cloud provider such as Dropbox, Google Drive, SkyDrive, Survey Monkey etc.
INSTRUCTIONS: (e.g., https://name1.name2.org/mystudy/login.html)
The URL is in the address bar of your web browser (e.g., Internet Explorer (IE), Firefox, Chrome)
If you need additional assistance contact your department computer support or system administrator for assistance in answering this question.

- Who manages / supports this server or website (e.g., Health Systems Computing Services (HS/CS),ITS, third party)? _____
  - List how you contact this support (e.g., name, email, phone number): _____
- What kind of device will be used to connect to this website/server? (*examples include non-UVA desktop computer, smart phone app, drive, tablet, laptop,*)? _____

- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), departmental technology support group, self)? _____
- List how you contact this support (e.g., name, email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

- Will the data be transferred elsewhere? Yes ☐ No ☐
  If yes, answer the following four questions.

  1. Will the data be transferred in an **encrypted** secure manner such as the use of SFTP or HTTPS? Yes ☐ No ☐
     1a. Describe the transfer method: _____

  2. How long will the data remain on the website/server before being transferred?_____

  3. Please provide the location the data are transferred to:_____

Data Security Plan: APPENDIX 1B(2) continued

4. After information is transferred elsewhere will all the data be **securely** delete from the website/server? Yes ☐ No ☐

- **NOTE: Securely** deleted means the data are overwritten with zeros and ones and then deleted. You may need to check with the website/server administrator about their deletion method.

- Will anyone other than study team members have access to data on the server/website? Yes ☐ No ☐
  - If yes, describe: _____

- Are any backups made of the information on the secure server/website? Yes ☐ No ☐
  If yes, explain how backups are made and where they are stored: _____

- Do the owners of the website/server have any rights to use or access data either individually or in aggregate? Yes ☐ No ☐
  If yes, please explain: _____

- If the website/server is not hosted at UVa, is there a Business Associates Agreement (BAA) with the provider of the non-UVa website? Yes ☐ No ☐ N/A ☐

END OF APPENDIX 1B(2)

Data Security Plan: APPENDIX 1B(3)

1B(3). To a UVa server NOT listed under 1B(4) below.

- Provide the name of the server/drive:_____

- Who manages / supports this server or website (e.g., Health Systems Computing Services (HS/CS),ITS, your department, third party)? _____

- List how you contact this support (e.g., name, email, phone number): _____

- What kind of device will be used to connect to this server/drive? _____
  (*examples include desktop computer, smart phone app, tablet, laptop,*?

- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), self)? _____

- List how you contact this support (e.g., name, email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

END OF APPENDIX 1B(3)

Data Security Plan: APPENDIX 1B(4)

1B(4). Directly to one or more of the UVa servers listed below.

- ☐ domatlas.eservices.virginia.edu
- ☐ dom-titan.eservices.virginia.edu
- ☐ Elson1.studenthealth.virginia.edu
- ☐ EPIC
- ☐ es3.eservices.virginia.edu
- ☐ gcrcserver.itc.virginia.edu
- ☐ \\HSCS-ss7
- ☐ \\HSCS-ss8
- ☐ \\HSCS-ss9
- ☐ \\HSCS-ss10
- ☐ \\HSCS-ss11
- ☐ \\HSCS-ss12
- ☐ \\HSCS-ss13
- ☐ \\hscs-share1\
- ☐ \\hscs-share2\
- ☐ \\hscs-share3\
- ☐ hstsdatalab.hscs.virginia.edu
- ☐ hstsdsmpogapp.hscs.virginia.edu
- ☐ Ivy Secure Computing Platform/ Ivy Secure Cloud/Ivy Cloud
- ☐ musicvpn01.med.virginia.edu
- ☐ Oncore (oncore.med.virginia.edu)
- ☐ School of Nursing SECURE NETf
- ☐ Redcap-int.hscs.virginia.edu
- ☐ \\radshare\
- ☐ upgusers.hscs.virginia.edu

- What kind of device will be used to connect to this server/drive? (*examples include desktop computer, smart phone app, tablet, laptop)* _____

- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), self)?_____

- List how you contact this support (e.g., name, email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

END OF APPENDIX 1B(4)

Data Security Plan: APPENDIX 1B(5)

1B(5).

Directly to a server/drive managed by the sponsor or CRO. Data must be sent and stored in an encrypted fashion (e.g. must be shared and stored via Secure FX, Secure FTP, HTTPS, PGP) and the server/drive is configured to store data regulated by HIPAA.

- Provide the name of the server/drive: _____
- What kind of device will be used to connect to this server/drive? (*examples include desktop computer, smart phone app, tablet, laptop,)*)? _____
- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), departmental technology support group, self)? _____
- List how you contact this support (e.g., name, Email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

END OF APPENDIX 1B(5)

Data Security Plan: APPENDIX 1C(2)a

1C(2)a. Storage of data *ONTO** an individual-use device (*examples include desktop computer, smart phone app, flash (thumb) drive, external hard drive, tablet, laptop, CD, C drive of your computer)*)

INSTRUCTIONS: *If you will store health information with any of the identifiers checked in the table 1C(1)a (around page 5) you must also complete and have signed a* ***Highly Sensitive Data Storage Request form available at:***
www.virginia.edu/informationsecurity/highlysensitivedata/approvalform.doc

- What kind of device is it (e.g. desktop computer, smart phone app, flash (thumb) drive, tablet, laptop, CD, C drive of your computer) _____
- Who manages / supports the device (e.g., Health Systems Computing Services (HS/CS), local computer support partner (LSP), self)? _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage:
http://www.virginia.edu/informationsecurity/device-requirements.html

- Will anyone other than study team members have access to data on the device?
  Yes ☐ No ☐ If yes, describe: _____
- Are any backups made of the information on the device? Yes ☐ No ☐
  - If yes, explain how backups are made and where they are stored: _____
- Does the owner of the device (e.g. phone service provider/ app developer) have any rights to use or access data either individually or in aggregate? Yes ☐ No ☐
- Are you storing audio- or video-recordings or pictures? Yes ☐ No ☐ N/A ☐
  - If yes, have you completed the Taping/Photography section in the protocol?
    Yes ☐ No ☐ N/A ☐
- If you are storing pictures or video recordings, do you confirm they will not include the full face?
  Yes ☐ No ☐ N/A ☐
- If you are storing audio- or video-recordings or pictures, do you confirm the data will not include HIPAA identifiers? Yes ☐ No ☐ N/A ☐

END OF APPENDIX 1C(2)a

Data Security Plan: APPENDIX 1C(2)b

1C(2)b. Storage of data on web-based or cloud storage (e.g., UVaBox, UVaCollab, online surveys or any cloud service)

- Provide the name of the website or cloud storage (e.g., URL): _____

NOTE: Not allowed if you have answered YES to any HIPAA identifier (the use of a unique subject ID (e.g. Subject # 1) is acceptable).

NOTE: No research data of any kind may be stored in a non-UVa licensed cloud provider such as Dropbox, Google Drive, SkyDrive, Survey Monkey etc.

INSTRUCTIONS: (e.g., https://name1.name2.org/mystudy/login.html)
The URL is in the address bar of your web browser (e.g., Internet Explorer (IE), Firefox, Chrome)
If you need additional assistance contact your department computer support or system administrator for assistance in answering this question.

- Who manages / supports this server or website (e.g., Health Systems Computing Services (HS/CS), ITS, third party)? _____
- List how you contact this support (e.g., name, email, phone number): _____
- What kind of device will be used to connect to this server/website? (*examples include desktop computer, smart phone app, tablet, laptop,*)? _____
- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), departmental technology support group, self)? _____
  - List how you contact this support (e.g., name, Email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

Data Security Plan: APPENDIX 1C(2)b continued

- Will anyone other than study team members have access to data on the server/drive?
  Yes ☐ No ☐
  - If yes, please describe: _____

- Are any backups made of the information on the secure server/drive? Yes ☐ No ☐
  If yes, explain how backups are made and where they are stored: _____

- Do the owners of the website/server have any rights to use or access data either individually or in aggregate? Yes ☐ No ☐
  If yes, please explain: _____

- If the website/server is not hosted at UVa, is there a Business Associates Agreement (BAA) with the provider of the non-UVa website? Yes ☐ No ☐ N/A ☐

END OF APPENDIX 1C(2)b

Data Security Plan: APPENDIX 1C(2)c

1C(2)c. To a UVa server NOT listed in 1C(2)d below.

- Provide the name of the server/drive: _____
- Who manages / supports this server or website (e.g., Health Systems Computing Services (HS/CS), ITS, third party)? _____
  - List how you contact this support (e.g., name, email, phone number): _____
- What kind of device will be used to connect to this server/drive? (*examples include desktop computer, smart phone app, tablet, laptop)*? _____
- Who manages / supports this individual-use device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), self)? _____
  - List how to contact this support (e.g., name, Email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

END OF APPENDIX 1C(2)c

Data Security Plan: APPENDIX 1C(2)d

1C(2)d. Directly to one or more of the UVa servers listed below.

- ☐ domatlas.eservices.virginia.edu
- ☐ dom-titan.eservices.virginia.edu
- ☐ Elson1.studenthealth.virginia.edu
- ☐ EPIC
- ☐ es3.eservices.virginia.edu
- ☐ gcrcserver.itc.virginia.edu
- ☐ \\HSCS-ss7
- ☐ \\HSCS-ss8
- ☐ \\HSCS-ss9
- ☐ \\HSCS-ss10
- ☐ \\HSCS-ss11
- ☐ \\HSCS-ss12
- ☐ \\HSCS-ss13
- ☐ \\hscs-share1\
- ☐ \\hscs-share2\
- ☐ \\hscs-share3\
- ☐ hstsdatalab.hscs.virginia.edu
- ☐ hstsdsmpogapp.hscs.virginia.edu
- ☐ Ivy Secure Computing Platform/ Ivy Secure Cloud/Ivy Cloud
- ☐ musicvpn01.med.virginia.edu
- ☐ Oncore (oncore.med.virginia.edu)
- ☐ School of Nursing SECURE NETf
- ☐ Redcap-int.hscs.virginia.edu
- ☐ \\radshare\
- ☐ upgusers.hscs.virginia.edu

- What kind of device will be used to connect to this server/drive? (*examples include desktop computer, smart phone app, tablet, laptop.)* _____

- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), self)? _____

  - List how to contact this support (e.g., name, email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

END OF APPENDIX 1C(2)d

Data Security Plan: APPENDIX 1C(2)e

1C(2)e. Directly to a server/drive managed by the sponsor or CRO. Data must be sent and stored in an encrypted fashion (e.g. must be shared and stored via Secure FX, Secure FTP, HTTPS, PGP) and the server/drive is configured to store data regulated by HIPAA.

- Provide the name of the server/drive: _____
- Who manages / supports this server or website? _____
- List how you contact this support (e.g., name, email, phone number): _____
- What kind of device will be used to connect to this server/drive? _____
  (*examples include desktop computer, smart phone app, tablet, laptop,)*)?

- Who manages / supports this device (e.g., Health Systems Computing Services (HS/CS), local computer support person (LSP), departmental technology support group,, self)? _____
- List how to contact this support (e.g., name, email, phone number): _____

INSTRUCTIONS: If the device is managed/support by *self* you must follow both the setup and maintenance security standards described on the UVa Office of Information Security, Policy & Records Office (ISPRO) webpage: http://www.virginia.edu/informationsecurity/device-requirements.html

END OF APPENDIX 1C(2)e

Data Security Plan Glossary:

Data Collected or Received: Where you put any kind of data recorded or gathered from another source for purposes of research. The data can come from any source, electronic, paper or voice. You may be sent these individual data points by paper, subject/patient interview or electronically. You may be manually extracting these data points from EPIC. You may be collecting these data with devices (camera, heart monitor, etc.)

Data Stored Long Term (Data storage) is different from data collected as it implies a longer-term non-volatile storage. It may be the same location as collected, (such as paper or HSCS server) or it may be a new location (computer drive or paper). It is where it is located for further analysis, manipulation, and access.

Highly Sensitive Data: includes personal information that can lead to identity theft if exposed and/or health information that reveals an individual's health condition and/or history of health services use. Electronic data storage policy: http://uvapolicy.virginia.edu/policy/IRM-015
Three HIPAA-identifiers are considered highly sensitive data by themselves (without being connected to PHI). These are #7-Social Security Number, #10-Account numbers, if it's a financial account number such as credit card or bank card number and #11 – Certificate/license number if it's a passport number, driver's license number, board license number, etc.). If these are in a file or on paper without any personal health information (PHI) it is still highly sensitive data (HSD).

Moderately Sensitive Data: includes information that is not highly sensitive nor is intentionally made public. So this category includes most of the data and information we work with. All research data that is not intentionally made public (e.g., published) is considered moderately sensitive data (MSD).

Individual Use Device: any kind of technology that has persistent memory. Flash memory, solid state drives, traditional hard drives, SD cards, USB thumb drives (sticks) allow for data to be kept long term. This means that any smartphones, laptops, tablets, biometric fitness devices and digital cameras and MP3 recorders (digital audio) qualify as individual use devices that could store potential data and must be protected.

Web based or Cloud storage: generally implies a storage server where a web browser is the main way to login and manipulate files. Sometimes a smartphone app is created to interface to these cloud storage containers. Examples include UVaBox, Box.com Google Drive, Google Docs, DropBox. Use of any Google Drive, Doc, Email, etc. for any UVa data or files is against UVa data protection policies.