**Social and Decision Analytics Division**

**Handling of**

**“Highly Sensitive and Proprietary Information”**

Data received from Social and Decision Analytics Division (SDAD) partners and all analysis of the data fall into the classification of highly sensitive and proprietary information.

In general, information is considered highly sensitive if disclosure would **seriously** undermine effectiveness of staff, and cause **significant** embarrassment or impact on corporate or sponsor assets or operations requiring **major** corrective action. This includes contractually or legally restricted information.

Examples of highly sensitive and proprietary information include:

* Information produced for or provided by a sponsor or partner that may be viewed only by named individuals (including PHI or work products created from PHI).
* Material that a sponsor or partner has requested be tightly restricted.
* Employee health information.
* Social Security numbers.
* Password files.
* Intellectual property requiring protection against unauthorized use (SDAD proprietary).

Release statements associated with highly sensitive and proprietary information include:

* Proprietary.
* Restricted: Highly Sensitive Personal Information.

# Highly Sensitive and Proprietary Information

The nature of SDAD’s technical work involves the use of external proprietary information obtained from federal, state, and partners from the healthcare industry or other third-party industry organizations as well as SDAD-owned proprietary information. To protect SDAD’s business relationships and interests, employees participating in these initiatives must handle proprietary information appropriately to avoid unauthorized disclosure to third-parties and anyone outside of SDAD who is not approved by the SDAD leadership team.

When SDAD accepts information designated “Highly Sensitive and Proprietary,” both the University and its employees are legally and ethically bound to safeguard it properly and to ensure that any disclosure of the information follows the directives furnished by the owner. In the absence of instructions from the owner, highly sensitive and proprietary information will be handled in accordance with the information below. SDAD’s continued access to highly sensitive and proprietary information depends on strict adherence to this policy.

In addition to handling highly sensitive and proprietary information in a manner consistent with our policies and procedures, additional requirements exist for our partners and will be specified in each set of legal agreements.

**General Requirements**

Highly sensitive and proprietary information will be handled on a Need to Know basis and will be restricted to SDAD members specified in writing pursuant to our partner agreements and SDAD policies and procedures. The named individuals of this small group will have access to the PHI data and the results of our analysis. The results will not be discussed with other SDAD employees or anyone outside of our small group including leadership and oversight not specifically name and authorized. All authorized ‘named individuals’ will be maintained by the research project lead and kept in a central location. (TBD)

Check List:

* All SDAD team members with access to highly sensitive and proprietary information are listed as ‘named individuals’.
* All SDAD team members with access to highly sensitive and proprietary information have signed a Non-Disclosure Agreement Propriety. (TBD).
* All SDAD team members with access to highly sensitive and proprietary information have undergone Security and HIPAA training as defined by the data storage team. (TBD)
* All SDAD team members with access to highly sensitive and proprietary information will complete the Health Research Quiz (Appendix D) prior to access and will complete the Quiz on an annual basis. (TBD)

The following sections include materials concerning the security protocols for individuals who are authorized users and viewers of the highly sensitive and proprietary information. Appendix A is an orientation to the security protocols including specific protocols for Sample Hospital (see Appendix B) and subsequent partners (see Appendix C).

**Appendix A**

**Orientation for Safe Handling of Highly Sensitive and Proprietary Information**

Highly sensitive and proprietary information will be handled in ways described in agreements between SDAD and provider partners. The following is a description of the expected procedures and protocols when handling highly sensitive and proprietary information. The goal of this orientation is to establish a culture of data security among the SDAD team.

Building a culture of data security begins with each individual. It is important to remember that we are granted *privileged* access to very personal and very confidential information. We must, at all times, respect the rights of the individuals whose information comprises the safety events from our provider partners as well as the cumulative information of all of the safety events.

Access to this information carries an immense responsibility and we must individually be trustworthy of this access and carefully guard the information. At some point we will all have the opportunity to break this trust. Health research is a hot issue these days and many will be interested in the work that we do. Our work is likely to reinforce news headlines and we might be tempted to share what we are learning outside of our small team. It may be tempting to discuss what you have heard or seen but you are always expected to resist this temptation and never disclose what you have learned through your privileged access beyond those who have a need to know.

We must hold ourselves and our team to the highest standard. SDAD and our health research is built on the premise that we will aggregate data from disparate sources to better analyze and understand those safety issues that impact out healthcare system. Therefore, it is imperative to remain a trusted steward of this data to achieve this overarching goal. The following section outlines specific work protocols that must be adhered to at all times when accessing highly sensitive and proprietary information.

**SDAD Rules of Behavior**

*Insert language regarding data handling…* All team members must complete the health research quiz after reading these orientation materials. The following sections contain information about the specific agreements with our partners. These are for reference only as all of the *safe data handling and Security and Privacy*. Appendices E and F contain specific protocols for day to day operations.

**Appendix B**

**Data Handling Protocols for Data from Sample Hospital**

## Overview of Agreement with Sample Hospital (Sample)

SDAD and Sample Hospital have entered in a Memorandum of Understanding (MOU) for the purpose of addressing significant healthcare related issues and to pursue through mutual interest in health research.

**Period of Performance**

Effective for \_\_ years starting on \_\_\_\_\_\_.

**Handling of Health Information**

The health information will include Sample Hospital non-sensitive information, as well as information in the form of Personally Identifiable Information (PII), Protected Health Information (PHI), and other highly sensitive and proprietary information. Sample Hospital is committed to respecting patient privacy and protecting the confidentiality and security of patient health and Sample Hospital information; as such, the health information will be handled with the following protocols:

* All personnel with authorized access will undergo HIPAA training and will comply with the rules of behavior.
* SDAD agrees not to disclose or use the PHI in any way other than expressly permitted by the agreement with Sample Hospital.
* Highly sensitive and proprietary information will be hosted in a dedicated and secured enclave located on \_\_\_\_\_ and this location meets all the HIPAA Security Regulations.
* Highly sensitive and proprietary information will be protected in accordance with the SDAD Security and Privacy Program and in coordination with Information Security.
* SDAD shall ensure that Sample Hospital highly sensitive and proprietary information is segregated from the SDAD network and from other information by hosting project resources in dedicated environments.
* SDAD agrees to report to Sample Hospital any disclosure of information in violation with the agreement as soon as possible but no later than 48 hours after becoming aware of the disclosure (including information about whose PHI was unsecured or unlawfully disclosed).
* In the event that Sample Hospital highly sensitive and proprietary information must be transported or stored on portable media of any type, the media shall be encrypted in accordance with FIPS 140-2 using AES-256 encryption.
* At the completion of our joint research or upon direction from Sample Hospital, SDAD shall sanitize media containing Sample Hospital highly sensitive and proprietary information by clearing and purging, as defined by NIST SP 800-88 “Guidelines for Media Sanitization.” SDAD shall notify Sample Hospital that the Sample Hospital data is destroyed.

**Relevant Requirements, Rules and Laws**

* FISMA, NIST, and HIPAA requirements.
* FIPS-199, Security Categorization for this highly sensitive and proprietary information shall be designated as Moderate for Confidentiality, Moderate for Integrity, and Low for Availability.
* NIST Special Publication 800-53 Rev 3.
* The Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules.
* The Health Information Technology for Economic and Clinical Health Act (HITECH) Act for implementing a security control baseline for the Security Categorization.

**Appendix C**

**Blank Form**

**Intentionally Left Blank**

**Appendix D**

**SDAD Security Training Quiz**

1. You are home visiting family and your parents ask you what you are working on these days. You mention that you are working on identifying patient safety risks by gathering patient safety information from different healthcare organizations. Your mom says that reminds her of a situation her friend experienced and she wants to know if you have seen things like that come up in your work. How do you respond:
   1. Pull up your access to the data and see if you can find a similar scenario.
   2. Tell your mom that you although would like to be able to talk about this you can’t share that information because you have to respect these patients’ right to privacy.
   3. Tell your mom you have seen some situations like that but that but only at specific hospitals.
   4. Request permission from your PL to show your mom this information.
2. At a conference, you run into an old friend who is working with a healthcare organization. They are interested in the work you are doing with health research and want to know if you can share some information about a competitor that has shared data with the program.
   1. You provide them with a point of contact with the SDAD research that will allow them visitors access to the data set for their competitor.
   2. Tell them that you can look up their competitor but only if they have a specific type of information in mind.
   3. Stop talking about the program immediately and change the subject.
   4. Tell them that you have an agreement to not discuss any of the partners that are involved in the program.
   5. Pretend like you don’t know much about who is a partner and that you aren’t involved enough with the program to know any of that information.
3. You receive a call from the Washington Post, they are doing a story on medical errors at a local DC hospital and they heard that SDAD is working on a patient safety initiative. They learned that you are involved in the project and they want to know if we have investigated this issue.
   1. Hang up the phone immediately.
   2. Pretend that you are not on the project and you don’t know if anyone who is.
   3. Refer them to the SDAD Leadership team and say that you are unable to comment any further.
   4. Refer them to corporate communications.
4. After an approved study was completed, you accidently discover that you had inadvertently left some highly sensitive and proprietary information on your laptop – what do you do?”
   1. Call The Washington Post and tell them that you have it.
   2. Pretend that you don’t have it and leave it on the laptop.
   3. Contact the hospital and ask them what to do with it.
   4. Delete the data as quickly as possible following the prescribed procedures.
5. You have been asked to provide a presentation at a UVA Knowledge Sharing Session on health research analysis where only UVA faculty and potential sponsors attend. For the presentation you would like to showcase all the great work you and other colleagues have been working on. You take a screen capture of some the Aggregate Metrics and one of the hospital’s safety benchmarks from our joint research, but are careful to not show the name of the hospital. You feel great that you are helping to share lessons learned and that you are facilitating the understanding of safety issues to the rest of UVA and some of the potential sponsors that will be there.
   1. You don’t need any permission because you were careful not to show the hospital.
   2. Re-design the presentation with “mock” data and get department management permission for the presentation.
   3. You need to get the hospital’s approval for your graphics.
   4. You need to get approval from your project leader, and show them the slides before your briefing.
   5. It is too hard to get permission, so you draw the dashboard with crayons.
6. One of your friends is a personal injury attorney. One day he begins asking you lots of questions about the SDAD health research, the types of data to which you have access, and the agreements we have with hospitals. You:
   1. Feign ignorance and say “I have no idea…”
   2. Answer his questions about the program in general terms without violating non-disclosure agreements.
   3. Refer him to the hospital’s POC then stop talking.
   4. Step away from the attorney.
7. Highly sensitive and proprietary information is going back and forth over encrypted e-mail between a very specific set of teammates who have access to the data. Then someone at a higher level who does not have access, requests information about the topic
   1. You forward the e-mail chain that was encrypted to the person who does not have authority to view the data.
   2. You don’t forward the chain of e-mails but you tell them a synopsis of the findings from the data.
   3. Invite them to view the data over your shoulder in your office.
   4. Refer them to the SDAD Leadership team.
8. You just conducted an analysis of safety event data as directed by your project leader. While at lunch with a friend from SDAD, you start to discuss what the friend is working on. You realized that findings from your analysis could have a major impact on your friend’s project in support of their customer’s work. Do you –
   1. Discuss what was in the study with your friend, speaking softly so no one at the next table can hear.
   2. Help your friend draft a request for information from the health research project for approval by the project leader.
   3. Send your friend a copy of the Executive Summary based on the analysis because it’s approved by your project leader.
   4. Have your friend invite you to their internal team meeting where you can brief on the findings of your analysis.
9. You see a report on the nightly news about an incident involving a hospital that has shared information with the health research project. Curious to learn more about the event, you decide to “investigate” further. Select the option that is acceptable for you to perform:
   1. Put other work aside and retrieve the relevant data from within SDAD for a quick analysis.
   2. Call the hospital’s health research POC’s and ask them for the details.
   3. Just take a quick peak at other hospitals’ data to see if there are any similar issues.
   4. Resist the temptation to analyze the event.
10. A representative from one of the hospitals involved with the health research calls you and requests a quick analysis of some patient safety data for a project he’s working on. You
    1. Drop everything since he’s an important sponsor, do the analysis and send him the results via email that day and let your project leader know afterwards.
    2. Get the OK from the SDAD Leadership team that this request has been logged and then get his approval before proceeding.
    3. Do the analysis and when your results look unique/odd send them out to a colleague to ask for their advice about how to proceed.
    4. After finding out that it is an official request approved by the project leader, do the analysis as a top priority. When your supervisor asks about other work, tell him that the sponsor’s request comes first.
11. You are meeting with a government financial regulatory agency, discussing with them the possibility of creating an research capability for tracking and preventing mortgage lending risks.  This could be a $20 million annual program for SDAD.  They would like to see how sharing highly sensitive and proprietary information across several organizations has helped to prevent errors and accidents in the airline industry. Do you:
    1. Send them the report of some safety event analysis from which the findings have been converted into Safety Enhancements.
    2. Inform your management of the request and let the requestor know someone will be in touch with a briefing and possible demonstration.
    3. Appease them with blandishments stating that “sharing is good” and “the hive mind sees and knows all,” but show nothing.
    4. Contact your project leader and ask for the topic to be put on the SDADleadership team agenda for approval.
12. You are on a deadline to send out a presentation to the SDAD health research team. This presentation includes aggregate information about Sample Hospital’s data along with a few excerpts from the free text data. You finish the presentation and need to head to a meeting quickly but your encryption token is not working. Do you:
    1. Send them the team the presentation anyway without encrypting it.
    2. Send it to a trusted teammate for them to send it to the entire team in an encrypted e-mail on your behalf.
    3. Call the help desk and use the “share-it” software while the presentation is open.
    4. Wait until you fix the issue to send the file in an encrypted e-mail while hoping everyone understands why the presentation is a bit delayed.