Life Hacks for Completing the IT Data Security Assessment Form Right the FIRST Time

Noreen L Connolly, MS, JD, CCRC
Senior Health Project Coordinator
Neurology/UR Epilepsy Center

Agenda – answering the questions – how to do it right

- ❑ What is the Electronic Data Security Assessment Form?
  (aka: Guideline for Human Subject Research Data Security Requirements - Appendix I – University of Rochester Human Subject Research Electronic Data Security Assessment Form; IT Data Security Form; 'The Form')
- ❑ When do I need to fill it out?
- ❑ Where do I find the Form?
- ❑ What information needs to be included?
- ❑ How do I obtain that information?
- ❑ What information do I put where on the Form?

IT Data Security Assessment Form

Data Security Form is all about protecting patient information (Data) – *that is:*

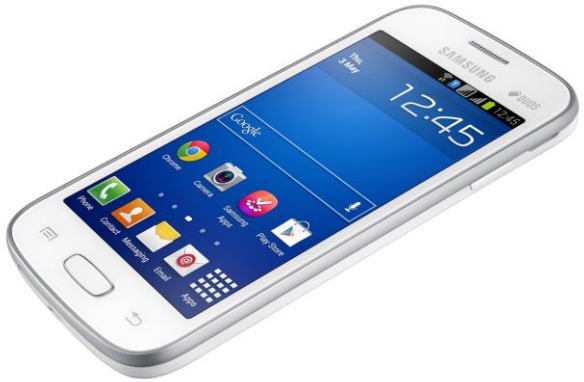
- Collected **electronically** from subjects
- Stored **electronically** and
- Transferred (shared) any where, to anyone –**electronically?**

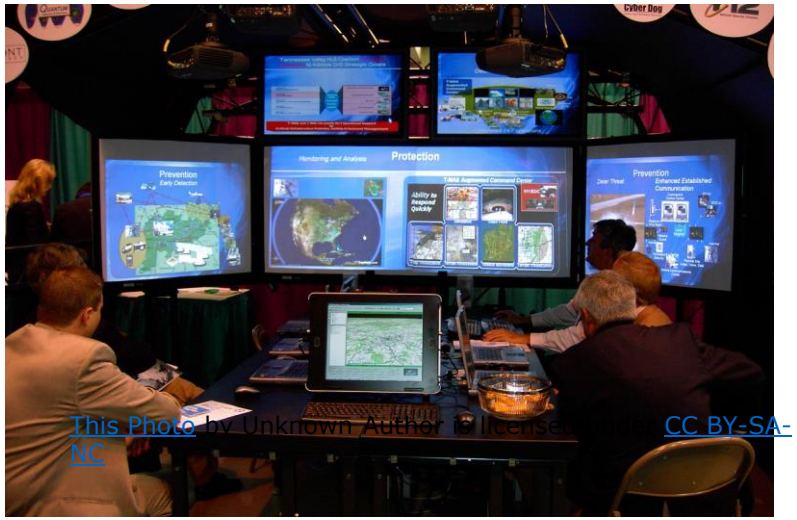
- Is that Subject data identifiable?

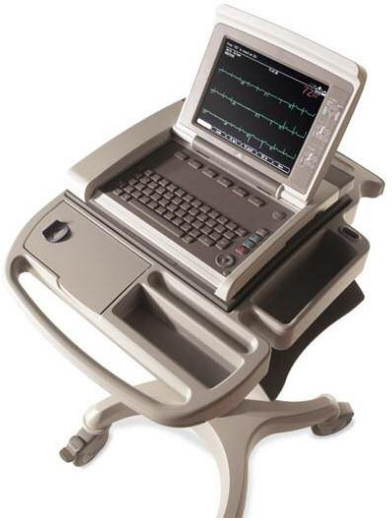
WHY??

Used to be:

Now:







When do I need to fill out the form?

- **For <u>every</u> RSRB submission -** to fill one out and submit with RSRB study approval package (even if ONLY paper CRFs!)
- **Some Data Use Agreements (DUA's) –** if the data sharing involves data that is stored on/in a UR database or computer and/or is going to be electronically shared may require one

Where do I find the form?

RSRB Page

↓

RSRB Information

↓

Policies & Guidelines

↓

1100 Miscellaneous Guidelines

↓

Data Security Assessment Form – Revised 05/2021

What do I need to know to fill out the form correctly??

Be able to categorize the subject data that is **collected, stored, processed or transmitted electronically**

Identify the devices are used to collect, store and transmit data electronically ***and***

Describe the protections in place to keep the subject data secure as it is collected, stored and transmitted.

Where do I get that formation?

BE PROACTIVE –about reportable items

Find out as early as possible what software, devices, websites, eDC, and other third party vendors are going to be used in the study

Review:

- First draft of a grant
- Protocol or Protocol synopsis
- Schedule of study tasks, imaging, diagnostic testing and assessments for hints on devices and 3rd party applications

Ask:

Your CRA at the Pre-Site Selection Visit for details on the technology that is going to be used:

- Are health assessments, survey data or diaries being collected on paper or collected on tablets or phones and electronically transmitted?

- Is the sponsor providing any devices –tablets, phones, wearables?

- Diagnostic testing: EEGs, ECGs, PET/CAT scans, MRIs being done - will we be transmitting this data to the sponsor -through a 3rd party vendor site?

Make a List

- Make a list of the **tools/devices/methods**, software that your study is using to **collect, store and share subject data electronically**

- **Type of data** – is PHI being collected, stored or transmitted electronically?
  - Is **identifiable** data being stored collected, stored or transmitted electronically?

Study System	Study System Details
EDC (Medidata Rave)	Data Capture
IWRS (Signant)	Randomization System
Central Lab (Lab Connect)	Lab Portal
Patient Travel/ Reimbursement	XXXXXX Patient Reimbursement Portal
Subject Recruitment (Praxis)	PI and SC will receive login to portal called “PraxisDirect.” All prequalified referral information will be stored here that is received from the digital recruitment campaign.
Signant Rater Training (Learning Zone)	Raters will receive their own log in and password for the Learning management system to complete their training.
Electronic Adjudication System (EAS) – Diagnosis Confirmation System	CISYS Is the name of the system
Central ECG Reader/ ECG Machine Supply (IQVIA Web Portal)	Spark Portal
Drug Dev (eConsent, site portal)	IQVIA Drug Dev system for e-consent & communication
IQVIA Study Hub (Virtual trials Platform)	The study hub is a secure platform for sites to connect with subjects/caregivers if the subject opts to do V6 and V8 remotely.

Items to include on the Devices List

P/Cs

Laptops

Tablets

ECG machine

MRIs/PET Scans/ECHO’s

Video EEG’s

Phones – data collection

Phones - texting

Are collection devices UR or Sponsor provided?

Actigraph watches, Fitbit

Wearable Cardiac monitors

In-home camera

ZOOM/TEAM visits

eDC –

Sponsor or Third party vendor, e.g. ert, SparkDev, IQIVIA Hub

Faxes

How is data being transferred? Is it secure?

Being proactive…about security

During the timeline discussions:

- Notify the study sponsor/CR that UR IT Security will need to do a security review of their eDC, Sponsor provided devices, apps and imaging upload/ storage system and that it can take several weeks.
- Request the name of their IT contact person(s) that will be responsible for providing the technical information.
- Ask for the 'Risk Assessment,' 'Data Security' or HIPAA Compliance information for all study apps, up/downloads and devices
- For **mobile devices**: need info on the MDM: Mobile Device Management: how is data collection and transfer made secure on the mobile device

Proactive: 3PA (third party assessment) for Vendor Vetting

Created to:

Evaluate ‘any third party that will be providing a device, service, application, consultation, network connectivity, data use, or data exchange at the University or Medical Center and affiliates’

Must use 3PA if:

- Identifiable subject data is being collected, stored or transmitted electronically–**needs 3PA before IT Data Security form**
- Device is being provided that involves connectivity – e.g., mobile devices

Proactive: 3PA (third party assessment) for Vendor Vetting

- A marked up copy of the 3PA Getting Started info that is found at https://tech.rochester.edu/services/3pa-third-party-assessment/), which is where you go to start the process. Then it walks you through how to access the actual application at (www.rochester.edu/it/3pa).

- 3PA Can be the first part of the IT Security Process is the 3PA submission: Start the 3PA process early - right after you have been awarded the study, and BEFORE reviewing the ICF. The 3PA review process can take 2-3 days or a couple of weeks.

You will receive the following email notifications:

Email telling you the application has been received and is in review.
An email notification from "The Third Party assessment" that says "vendor Request Status updated to "Manual Approval".

3PA- then IT Data Security Assessment Form

The second part of the IT Security Review Process is a form within the CLICK IRB system and is part of the CLICK Submission Process for a new study.

Best to complete and upload a scan of the Appendix I Form AND a <u>scan of the 3PA email approval email notification you have received</u> as part of your CLICK submission. This way the Data Security Form information is linked with the 3PA review approval.

Being proactive… about security

Email Mary Hallinan, Risk and Compliance Analyst, UR Information Security Office and ask

- if your vendor is on the 'vetted' list if you suspect it is.
- Do they see any 'red flags' in the list?
- Do you need a 3PA or not?
- Does this device need additional review due to network capabilities?

Mary_Hallinan@urmc.Rochester.edu

Mary and her team stress the 'evolving' nature of this whole process.
They want to help us get through this, GREAT to work with!!!

Let’s Look at the Form….

Hacks for Getting it Right!

1) Understand the purpose of the form
2) **Be proactive**
3) **Use 3PA** if you have identifiable PHI and device
4) **Fill out every section**
5) Provide explanation when clarity needed
6) Less is more – don't over-explain, add info not required
7) Use template language for those common scenarios/devices
8) Submit multiple forms for complicated studies
9) **Ask** if you aren't sure: CRA, Vendor, Mary Hallinan, your IT folks, Information Systems Division, Academic IT

UR
MEDICINE

MEDICINE *of* THE HIGHEST ORDER