Emory Office of Information Technology (OIT)

Security Review Process in Human Subject Research Studies

Mike (Mo) Davidson

Associate Director, Information Security Architecture

Topics:

Part 1

- Cyber Threat Landscape
- Examples of Sensitive Data
- Why Emory Cares About Data Security
- Preventing Data Breaches

Part 2

- Security Review Process in Human Subject Research Studies
- New Process Improvements

Topics:

Part 1

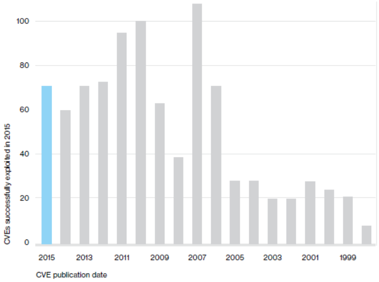
Cybersecurity Background Information

Cyber Threat Landscape

Sophisticated and Motivated Actors

Exploitation of the Internet of Things

Rise of Advanced Ransomware Threats



Attacks Continue to Target Old Vulnerabilities

1.1 Billion

Records Breached

In U.S. Since 2005

16.7 Million

Identity Theft Victims per Year

$16.8 Billion Stolen

Cyber Threat Landscape

Phishers/Spammers

Malware

Financial Fraudsters

Nation States

Primary Threat Actors

1000
Unique Attackers

Identified and Quarantined Every Month

235 Million
Malicious Communications

Blocked Every Month

4 Major Incidents & 315 Minor Incidents

Last 12 Months

Examples of Sensitive Data

- Identifiable Electronic Protected Health Information (ePHI).
- Individually Identifiable Health Information (IIHI)
- Human subject research data containing Personally Identifiable Information (PII)
- Combinations of Personally Identifiable Information that could readily be used for identity theft:
  - Social security numbers, when combined with any form of the corresponding name
  - Driver's license numbers, when combined with any form of the corresponding name
- Non-directory student information
- Passwords
- Credit/Debit card numbers
- Financial records that could lead to identity theft or fraud
- Any data deemed to be restricted by the data owner
- Any data that, if acquired by unauthorized individuals would require notification of affected parties
- Any data that Emory is legally, contractually, or ethically obligated to encrypt

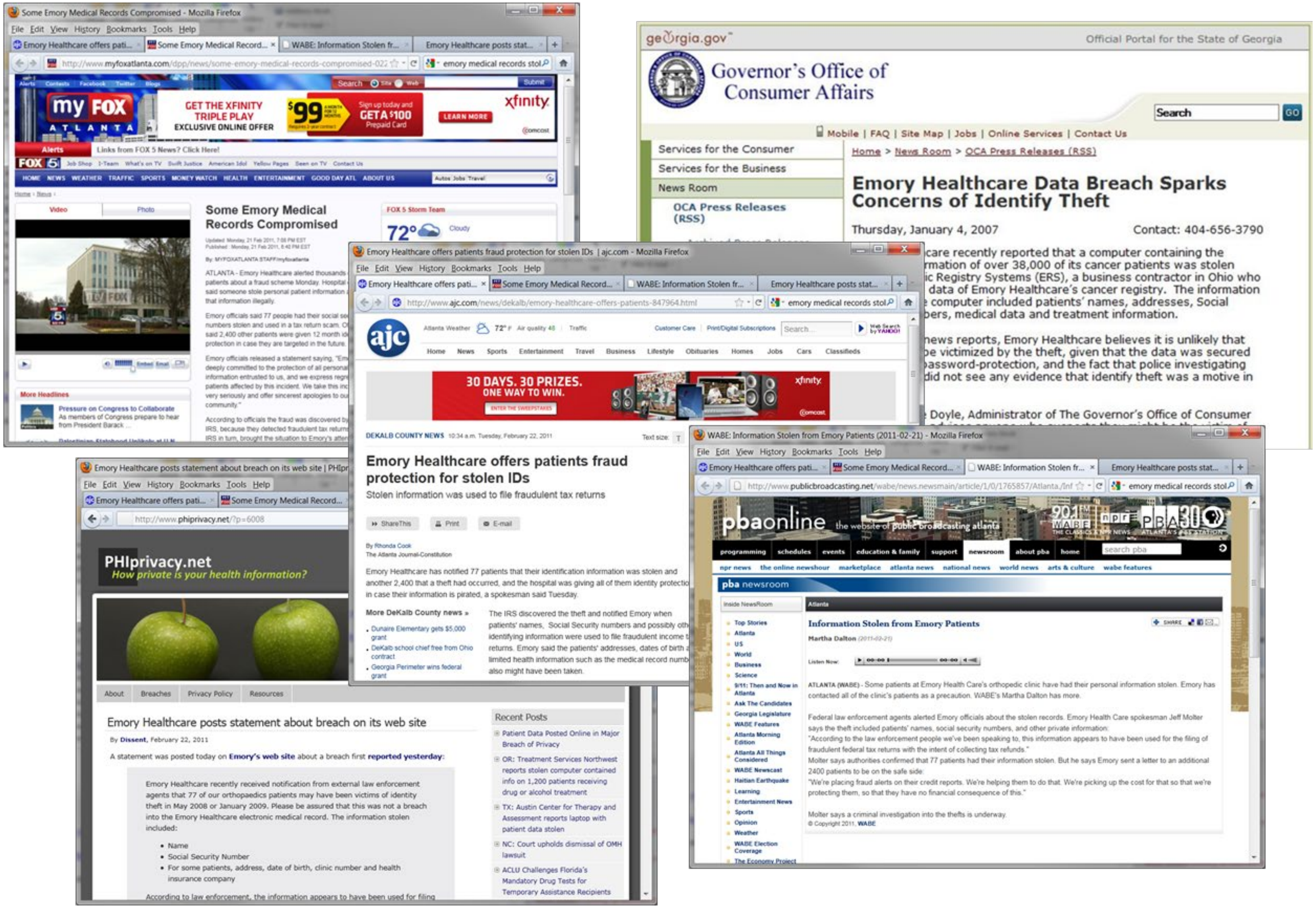
Why Emory Cares About Data Security

- It’s the law (HIPAA, FERPA, PCI, etc.)
- Financial Impact

Forensic analysis	$5K to $15K per system
Notifying affected parties	$1 per individual
Credit monitoring	$6 per individual
Fines and Penalties	Can easily exceed $1,000,000
Lawsuits	Unlimited

  - Incident costs are allocated to the department where the breach occurred
- Damage to Institutional Reputation
  - Negatively affects recruitment of faculty and students
  - Negatively affects fundraising
  - Could negatively affect ability to get grants
  - Negatively affects the willingness of other institution to share sensitive data
- Breach of computer security / confidentiality identified as one of Emory’s top risks during every Enterprise Risk Management assessment

Why Emory Cares About Data Security


Some Emory Medical Records Compromised - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Emory Healthcare offers pati... | Some Emory Medical Record... | WABE: Information Stolen fr... | Emory Healthcare posts stat...
http://www.myfoxatlanta.com/dpp/news/some-emory-medical-records-compromised-022
emory medical records stol
my FOX ATLANTA
GET THE XFINITY TRIPLE PLAY EXCLUSIVE ONLINE OFFER
$99
Sign up today and GET A $100 Prepaid Card
LEARN MORE
xfinity
Alerts
Links from FOX 5 News? Click Here!
FOX 5
HOME NEWS WEATHER TRAFFIC SPORTS MONEY WATCH HEALTH ENTERTAINMENT GOOD DAY ATL ABOUT US
Video
Photo
FOX 5 Storm Team
72° Cloudy
More Headlines

Some Emory Medical Records Compromised

Updated: Monday, 21 Feb 2011, 7:08 PM EST
Published: Monday, 21 Feb 2011, 6:40 PM EST

By: MYFOXATLANTA STAFF/myfoxatlanta

ATLANTA - Emory Healthcare alerted thousands patients about a fraud scheme Monday. Hospital said someone stole personal patient information that information illegally.

Emory officials said 77 people had their social se numbers stolen and used in a tax return scam. O said 2,400 other patients were given 12 month id protection in case they are targeted in the future.

Emory officials released a statement saying, "Em deeply committed to the protection of all personal information entrusted to us, and we express regre patients affected by this incident. We take this inc very seriously and offer sincerest apologies to ou community."

According to officials the fraud was discovered by IRS, because they detected fraudulent tax returns IRS in turn, brought the situation to Emory's atten

Pressure on Congress to Collaborate
As members of Congress prepare to hear from President Barack ...

ge0rgia.gov
Official Portal for the State of Georgia
Search
GO
Mobile | FAQ | Site Map | Jobs | Online Services | Contact Us
Services for the Consumer
Services for the Business
News Room
OCA Press Releases (RSS)

Governor's Office of Consumer Affairs

Home > News Room > OCA Press Releases (RSS)

Emory Healthcare Data Breach Sparks Concerns of Identify Theft

Thursday, January 4, 2007 Contact: 404-656-3790

care recently reported that a computer containing the rmation of over 38,000 of its cancer patients was stolen ic Registry Systems (ERS), a business contractor in Ohio who data of Emory Healthcare's cancer registry. The information computer included patients' names, addresses, Social bers, medical data and treatment information.

news reports, Emory Healthcare believes it is unlikely that be victimized by the theft, given that the data was secured password-protection, and the fact that police investigating did not see any evidence that identify theft was a motive in

Doyle, Administrator of The Governor's Office of Consumer

Emory Healthcare offers patients fraud protection for stolen IDs | ajc.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Emory Healthcare offers pati... | Some Emory Medical Record... | WABE: Information Stolen fr... | Emory Healthcare posts stat...
http://www.ajc.com/news/dekalb/emory-healthcare-offers-patients-847964.html
emory medical records stol
ajc
Atlanta Weather 72° F Air quality 48 | Traffic
Customer Care | Print/Digital Subscriptions
Search...
Web Search by YAHOO!
Home News Sports Entertainment Travel Business Lifestyle Obituaries Homes Jobs Cars Classifieds
30 DAYS. 30 PRIZES. ONE WAY TO WIN.
ENTER THE SWEEPSTAKES
xfinity
Text size: T
ShareThis
Print
E-mail

DEKALB COUNTY NEWS 10:34 a.m. Tuesday, February 22, 2011

Emory Healthcare offers patients fraud protection for stolen IDs

Stolen information was used to file fraudulent tax returns

By Rhonda Cook
The Atlanta Journal-Constitution

Emory Healthcare has notified 77 patients that their identification information was stolen and another 2,400 that a theft had occurred, and the hospital was giving all of them identity protectio in case their information is pirated, a spokesman said Tuesday.

More DeKalb County news »
- Dunaire Elementary gets $5,000 grant
- DeKalb school chief free from Ohio contract
- Georgia Perimeter wins federal grant

The IRS discovered the theft and notified Emory when patients' names, Social Security numbers and possibly oth identifying information were used to file fraudulent income t returns. Emory said the patients' addresses, dates of birth a limited health information such as the medical record numb also might have been taken.

Emory Healthcare posts statement about breach on its web site | PHIpr
File Edit View History Bookmarks Tools Help
Emory Healthcare offers pati... | Some Emory Medical Record...
http://www.phiprivacy.net/?p=6008
PHIprivacy.net
How private is your health information?
About
Breaches
Privacy Policy
Resources

Emory Healthcare posts statement about breach on its web site

By Dissent, February 22, 2011

A statement was posted today on Emory's web site about a breach first reported yesterday:

> Emory Healthcare recently received notification from external law enforcement agents that 77 of our orthopaedics patients may have been victims of identity theft in May 2008 or January 2009. Please be assured that this was not a breach into the Emory Healthcare electronic medical record. The information stolen included:
>
> - Name
> - Social Security Number
> - For some patients, address, date of birth, clinic number and health insurance company
>
> According to law enforcement, the information appears to have been used for filing

Recent Posts
- Patient Data Posted Online in Major Breach of Privacy
- OR: Treatment Services Northwest reports stolen computer contained info on 1,200 patients receiving drug or alcohol treatment
- TX: Austin Center for Therapy and Assessment reports laptop with patient data stolen
- NC: Court upholds dismissal of OMH lawsuit
- ACLU Challenges Florida's Mandatory Drug Tests for Temporary Assistance Recipients

WABE: Information Stolen from Emory Patients (2011-02-21) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Emory Healthcare offers pati... | Some Emory Medical Record... | WABE: Information Stolen fr... | Emory Healthcare posts stat...
http://www.publicbroadcasting.net/wabe/news.newsmain/article/1/0/1765857/Atlanta./Inf
emory medical records stol
pbaonline the website of public broadcasting atlanta
90.1 FM WABE THE CLASSICS & NPR NEWS
npr
PBA30 ATLANTA'S PBS STATION
programming schedules events education & family support newsroom about pba home
search pba
npr news the online newshour marketplace atlanta news national news world news arts & culture wabe features
pba newsroom
Inside NewsRoom
Top Stories
Atlanta
US
World
Business
Science
9/11: Then and Now in Atlanta
Ask The Candidates
Georgia Legislature
WABE Features
Atlanta Morning Edition
Atlanta All Things Considered
WABE Newscast
Haitian Earthquake
Learning
Entertainment News
Sports
Opinion
Weather
WABE Election Coverage
The Economy Project
Atlanta
SHARE
Listen Now:

Information Stolen from Emory Patients

Martha Dalton (2011-02-21)

ATLANTA (WABE) - Some patients at Emory Health Care's orthopedic clinic have had their personal information stolen. Emory has contacted all of the clinic's patients as a precaution. WABE's Martha Dalton has more.

Federal law enforcement agents alerted Emory officials about the stolen records. Emory Health Care spokesman Jeff Molter says the theft included patients' names, social security numbers, and other private information:
"According to the law enforcement people we've been speaking to, this information appears to have been used for the filing of fraudulent federal tax returns with the intent of collecting tax refunds."
Molter says authorities confirmed that 77 patients had their information stolen. But he says Emory sent a letter to an additional 2400 patients to be on the safe side:
"We're placing fraud alerts on their credit reports. We're helping them to do that. We're picking up the cost for that so that we're protecting them, so that they have no financial consequence of this."

Molter says a criminal investigation into the thefts is underway.
© Copyright 2011, WABE

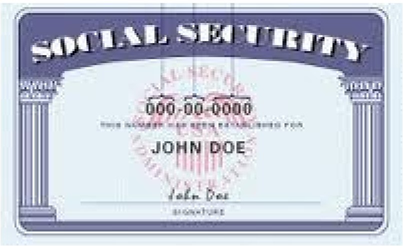
Why You Should Care About Data Security

- **Legal Consequences** – HIPAA contains criminal penalties for violating privacy requirements. Up to $250,000 fine and/or up to 10 years in jail.
- **Identity theft and financial fraud** – a compromised account could give an attacker access to your own Personally Identifiable Information.
- **Personal reputation** – breach notification letters are signed by leadership within the business unit where the breach occurs.
- **Data loss or corruption** – research data could easily be modified, destroyed or corrupted.

Preventing Data Breaches

- Ask your local IT support for help securing sensitive data

- Eliminate or minimize the use of SSN (and other sensitive data)
  - Use substitute identifiers
  - Truncate or Mask
  - Change business practices



- Move sensitive data to secure central storage solutions
  - Don’t store sensitive data on workstations, laptops, USB drives, smartphones, etc.

Preventing Data Breaches

Manning

Assange

- Tightly control who can access or modify sensitive data

- Ensure data transfer agreements are in place before transferring data to other institutions

- Delete old files that are no longer needed

- Encrypt Devices and Media
  - Laptops
  - Workstations that must store sensitive data
  - Servers
  - Removable media

Preventing Data Breaches

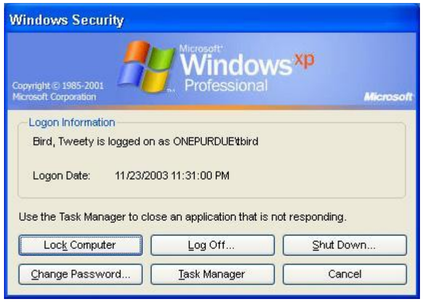
- Physically securing any systems or media containing sensitive information

- Never leave unsecured devices or paper containing sensitive information unattended
  - Especially in your car

- Choose a strong password, never share it with anyone else, and change it periodically

Preventing Data Breaches

- Log out, disconnect, or lock your workstation when you step away



Logon Information

Bird, Tweety is logged on as ONEPURDUE\tbird

Logon Date: 11/23/2003 11:31:00 PM

Use the Task Manager to close an application that is not responding.

- Backup your data to secure central storage solutions

- Shred, erase, or otherwise destroy paper records or electronic media containing sensitive data before disposing of them

Preventing Data Breaches

- Only send sensitive information via email if it is <u>encrypted</u>

- Don’t store sensitive data on unapproved external services like Google Docs, DropBox, Carbonite, IDrive, iCloud, etc.

- Ensure that appropriate audit logging is in place for sensitive data regardless of its location

Preventing Data Breaches

- Ensure that audit logs are regularly reviewed

- Ensure that your systems stay current on all patches and anti-virus updates

- Understand your obligations
  - Regulations
  - Policies (policies.emory.edu)
  - Grant and Contract requirements

LAWS & POLICIES

- NSPM-33: National Security Presidential Memorandum 33
  - National Security Strategy for United States Government-Supported Research and Development

National Science and Technology Council

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022

Preventing Data Breaches

- Complete all required security and privacy training
  - HIPAA Modules
  - NSPM-33 required cybersecurity training
  - Foreign Travel Requirements

- Use applications that have already been vetted for use with sensitive data
  - Search for “OIT Reviewed Apps” on the Emory home page
  - https://it.emory.edu/security/protecting-data/software_for_research.html

- Request a security scan or security review of your systems via ServiceNow

Topics:

Part 2

Security Review Process in Human Subject Research Studies

New Process Improvements

Security Review Process in Human Subject Research Studies

- In addition to the IRB review process, a security review may be conducted by the Office of Information Technology (OIT) Information Security Architecture Team

- An OIT Security Review could be needed:
  - If a study is using identifiable health data
  - If a study is handling sensitive data which may need some additional review to ensure the handling / storing / transmission is secure
  - If a study is using new technology

Security Review Process in Human Subject Research Studies

- Additionally, until a system or service has been vetted and added to the Approved for Research using Identifiable Information list, a security review will need to be conducted

- Finally, if the IRB identifies that there are any other parameters for a study that may warrant a closer look, the IRB may require an OIT Security Review be performed

Security Review Process in Human Subject Research Studies

- Documentation which may be requested in the course of a security review for IT components of an IRB study
  - Diagram of how the IT component will be used (architecture diagram)
  - Data flow diagram
  - Security questionnaires
  - Security info or attestations from IT vendors and medical device manufacturers
  - DUA / DTA / BAA
  - Evidence of encryption (in transit, at rest)
  - The study protocol

Security Review Process in Human Subject Research Studies

- Timeline / duration of a security review
- Depends on several factors but primarily:
  - Responsiveness from study team members / vendors for requested information
  - Accuracy of information provided to Security
  - Workload (in the request queue) for other security reviews being requested / worked on

- IRB approval will be pending until the completion of the security review

PENDING

Security Review Process in Human Subject Research Studies

- Typical order of activities for a security review
  - Security review request submitted via ServiceNow
  - Initial review by Security; request(s) for additional info
  - Q&A on aspects of IT solution / passed to vendor(s)
  - Clarification on diagrams / documents / usage
  - Clarification on data classifications (PHI vs IIHI)
  - Data flow identified / clarified (all Emory / 3rd party)
  - Potential information security risks identified in report
  - Preliminary Security Review Assessment Report shared
  - Risks either remediated / mitigated / accepted
  - Accepted risks signed off within document
  - Completed Security Review Assessment Report shared

Security Review Process in Human Subject Research Studies

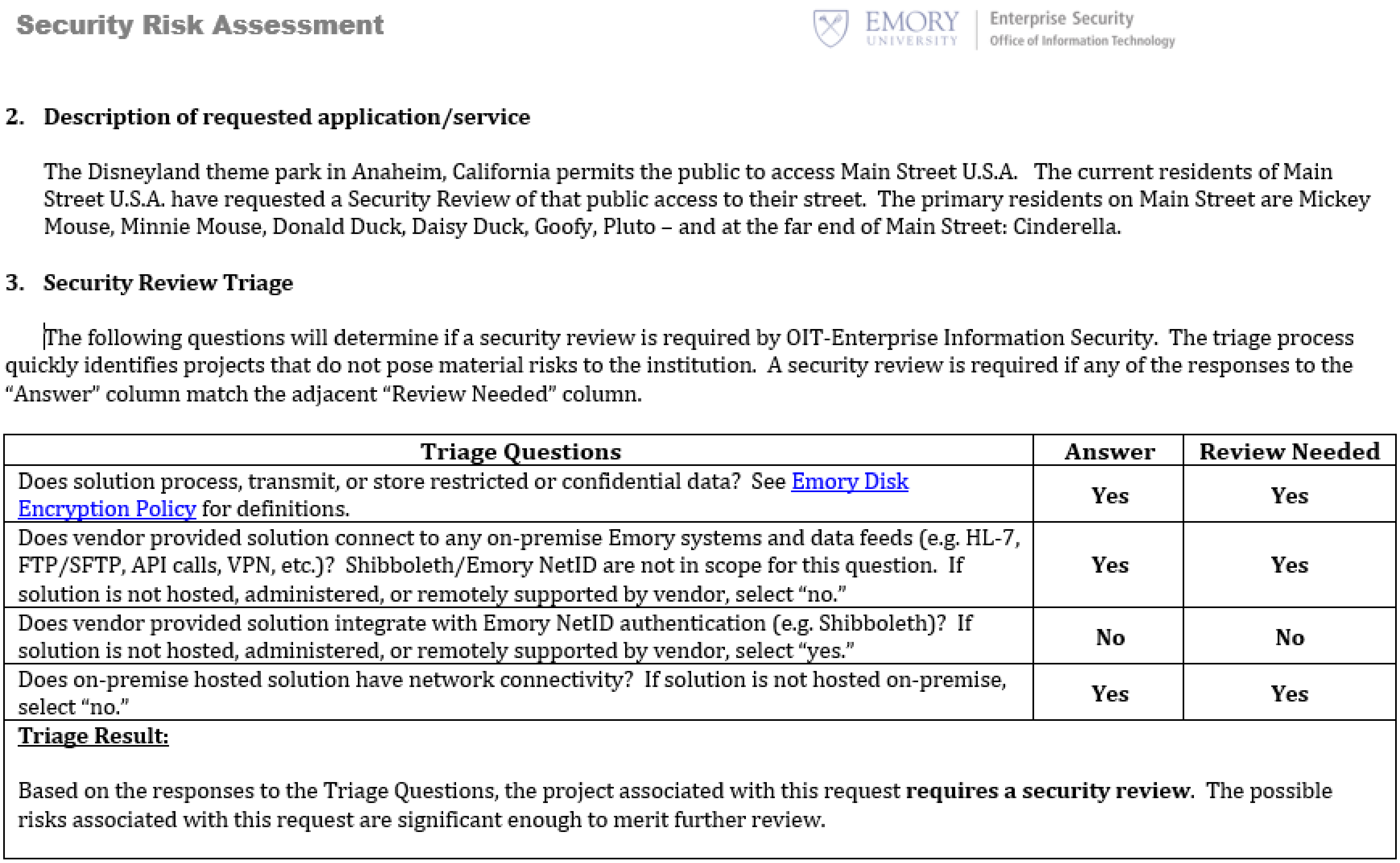
The following are screenshots of an example of an OIT Security Review Assessment Report

Security Risk Assessment

Risk Project Name:	**Request Number:**	**Prepared by:**	**Date:**
Disneyland Main Street U.S.A. public access	REQ # G00F33	Woody the Sheriff	July 17,1955
Division	**Business Unit:**	**Responsible Party**	**Requestor**
Disneyland – Anaheim, California	Main Street U.S.A.	Buzz Lightyear	Mickey Mouse

1. Risk level definitions, mitigation timelines, and risk acceptance criteria

Risk Level	Description	Mitigation Timeline	Risk Acceptance Criteria
Critical	The Security Review has determined that the current level of risk associated with the finding is **critical (severe)** in its current state.	The risk must be fully remediated or mitigated to an acceptable level within 30 days if system is live. If the system is not yet live, the risk must be fully remediated or mitigated to an acceptable level before the system goes live or is connected to a production Emory network.	Critical risks can only be accepted by Responsible Party such as VP/Dean level leadership. Relevant Executive VP level leadership must be informed that the risk is being accepted by the VP/Dean.
High	The Security Review has determined that the current level of risk associated with the finding is **high (substantial)** in its current state.	The risk must be fully remediated or mitigated to an acceptable level within 60 days if the system is live. If the system is not yet live, the risk must be fully remediated or mitigated to an acceptable level before the system goes live or is connected to a production Emory network.	High risks can be accepted by Responsible Party such as Director/Chair level leadership. VP/Dean level leadership must be informed that the risk is being accepted by the Director/Chair.
Medium	The Security Review has determined that the current level of risk associated with the finding is **medium (moderate)** in its current state.	The risk must be fully remediated or mitigated to an acceptable level within 90 days.	Medium risks may be accepted by Responsible Party such as Director/Chair level leadership.
Low	The Security Review has determined that the current level of risk associated with the finding is **low (tolerable)** in its current state.	Risk remediation is recommended, but not required at present.	Low risks do not need to be explicitly accepted.



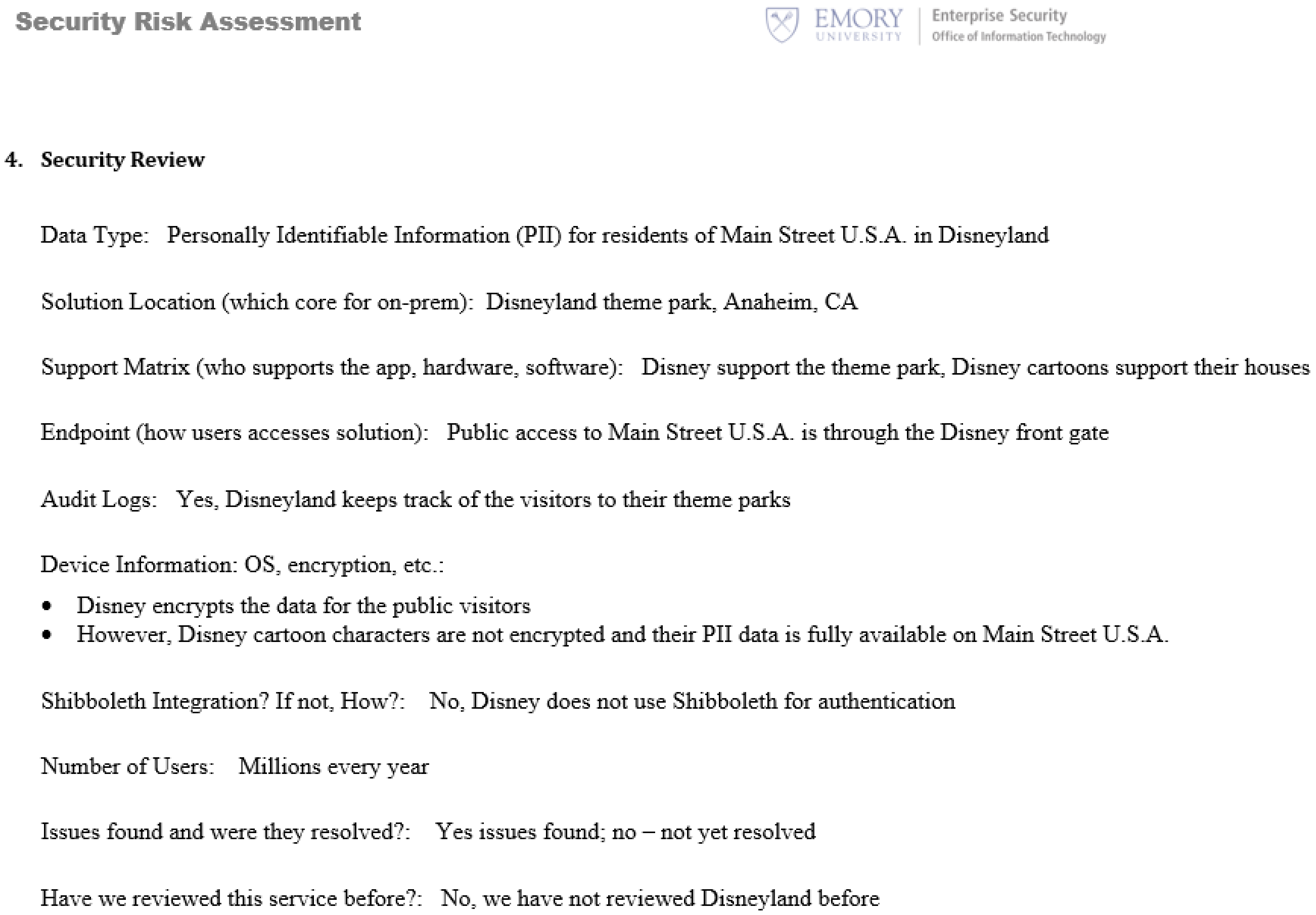
2. Description of requested application/service

The Disneyland theme park in Anaheim, California permits the public to access Main Street U.S.A. The current residents of Main Street U.S.A. have requested a Security Review of that public access to their street. The primary residents on Main Street are Mickey Mouse, Minnie Mouse, Donald Duck, Daisy Duck, Goofy, Pluto – and at the far end of Main Street: Cinderella.

3. Security Review Triage

The following questions will determine if a security review is required by OIT-Enterprise Information Security. The triage process quickly identifies projects that do not pose material risks to the institution. A security review is required if any of the responses to the "Answer" column match the adjacent "Review Needed" column.

Triage Questions	Answer	Review Needed
Does solution process, transmit, or store restricted or confidential data? See Emory Disk Encryption Policy for definitions.	**Yes**	**Yes**
Does vendor provided solution connect to any on-premise Emory systems and data feeds (e.g. HL-7, FTP/SFTP, API calls, VPN, etc.)? Shibboleth/Emory NetID are not in scope for this question. If solution is not hosted, administered, or remotely supported by vendor, select "no."	**Yes**	**Yes**
Does vendor provided solution integrate with Emory NetID authentication (e.g. Shibboleth)? If solution is not hosted, administered, or remotely supported by vendor, select "yes."	**No**	**No**
Does on-premise hosted solution have network connectivity? If solution is not hosted on-premise, select "no."	**Yes**	**Yes**
Triage Result: Based on the responses to the Triage Questions, the project associated with this request **requires a security review**. The possible risks associated with this request are significant enough to merit further review.		



4. Security Review

Data Type: Personally Identifiable Information (PII) for residents of Main Street U.S.A. in Disneyland

Solution Location (which core for on-prem): Disneyland theme park, Anaheim, CA

Support Matrix (who supports the app, hardware, software): Disney support the theme park, Disney cartoons support their houses

Endpoint (how users accesses solution): Public access to Main Street U.S.A. is through the Disney front gate

Audit Logs: Yes, Disneyland keeps track of the visitors to their theme parks

Device Information: OS, encryption, etc.:

- Disney encrypts the data for the public visitors
- However, Disney cartoon characters are not encrypted and their PII data is fully available on Main Street U.S.A.

Shibboleth Integration? If not, How?: No, Disney does not use Shibboleth for authentication

Number of Users: Millions every year

Issues found and were they resolved?: Yes issues found; no – not yet resolved

Have we reviewed this service before?: No, we have not reviewed Disneyland before

5. Risk Assessment Findings

THIS SECTION IS TO BE COMPLETED BY THE ENTERPRISE INFORMATION SECURITY TEAM

Enterprise Security Team member completes the section based on the submitted documentation and then sends the document to a Requestor/Responsible Party.

Risk Assessment Findings					
Item Number	**Risk Category**	**Findings**	**Findings Description**	**Recommended Remediation**	**Risk Level**
R-01	Data Protection	The public is allowed access to Main Street U.S.A. in Disneyland with all of the Disney characters PII data available / unencrypted	Public access has been available to Main Street U.S.A. but the PII data for the Disney cartoon characters has been left unencrypted by Disney.	Disneyland should encrypt the PII data for each of the cartoon characters who live on Main Street U.S.A.	**High**
		# No more risks found #			

6. Risk Mitigation Results

THIS SECTION IS TO BE COMPLETED BY THE REQUESTOR

This section is to be completed by a person who requested the review – Requestor along with the Responsible Party and then sent back to a member of the Enterprise Security Team.

Each of the risks documented in this section must be addressed in a manner that is consistent with the guidance provided in the table in section 1 and should be based on its associated risk level

Risk Mitigation Results				
Item Number	**Risk Description**	**Remediation approach**	**Estimated Completion Date**	**Name of Risk Owner(s)**
R-01	There needs to be assurance that Disneyland will encrypt the PII for the Disney cartoon characters who live on Main Street U.S.A.	Disney agrees to encrypt the PII data for all Disney cartoon characters who live on Main Street U.S.A. in Disneyland, California.	3 days before Infinity and Beyond	Buzz Lightyear (Representing Disney animators)

7. Residual Risk

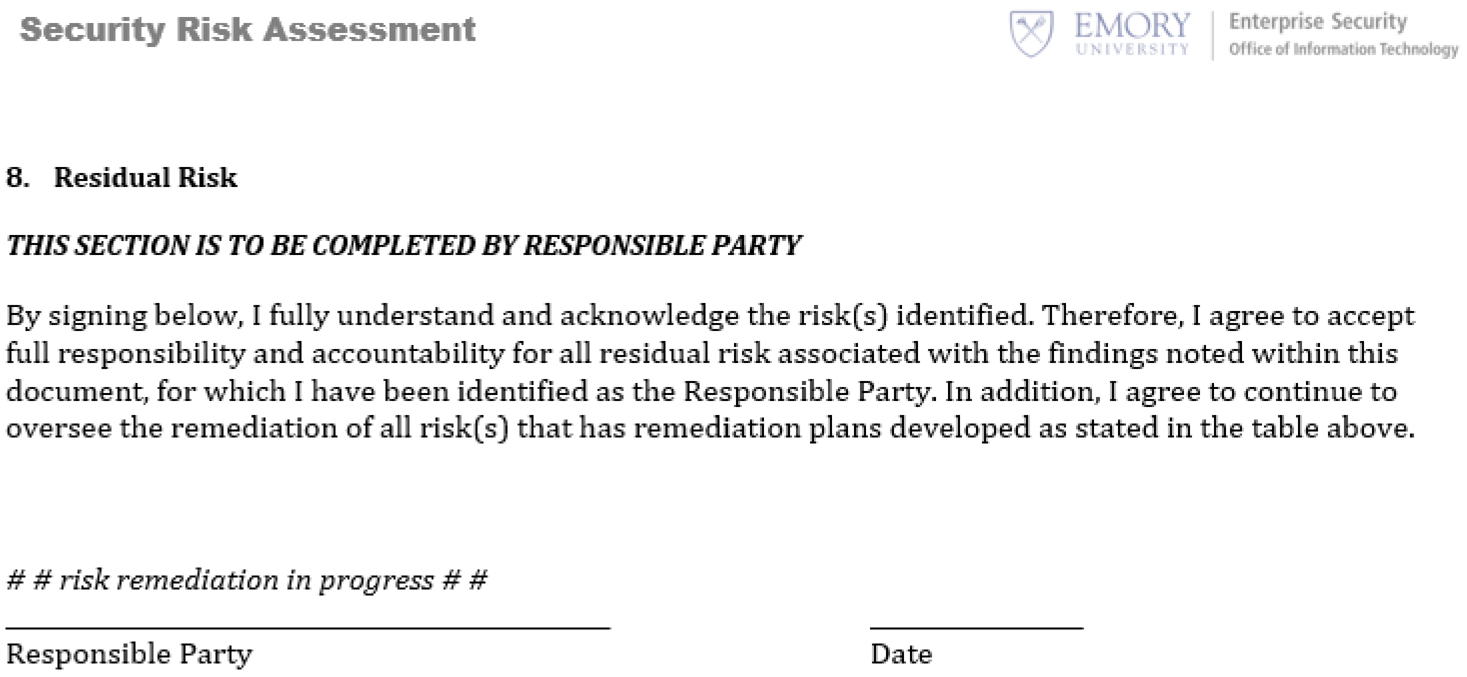
THIS SECTION IS TO BE COMPLETED BY THE ENTERPRISE INFORMATION SECURITY TEAM:

The member of the Enterprise Security Team reviews the mitigation efforts performed and classifies any residual risks in the table below and sends the update document to the Requestor/Responsible Party.

If any risk assessment finding is not fully remediated, any residual risk associated with the finding must be formally accepted by a Responsible Party -an organizational leader with sufficient authority to accept the risk given its residual risk level. Please refer to the table in section 1 in this document to identify the appropriate leader to fulfill this role.

Only one leader should fulfill the role of Responsible Party. The leader who is responsible for the highest residual risk(s) should sign off on all risks.

Item Number	**Risk Description**	**Residual Risk**	**Residual Risk Level**	**Residual Risk Action (Remediated, In Progress, or Accepted)**	**Risk Owner(s)**
R-01	There needs to be assurance that Disneyland will encrypt the PII for the Disney cartoon characters who live on Main Street U.S.A.	*Disney animators agree to encrypt the Disney cartoon characters PII data.*	***Low***	***In Progress***	**Buzz Lightyear** **(Representing Disney animators)**



Security Risk Assessment

EMORY UNIVERSITY | Enterprise Security
Office of Information Technology

8. Residual Risk

THIS SECTION IS TO BE COMPLETED BY RESPONSIBLE PARTY

By signing below, I fully understand and acknowledge the risk(s) identified. Therefore, I agree to accept full responsibility and accountability for all residual risk associated with the findings noted within this document, for which I have been identified as the Responsible Party. In addition, I agree to continue to oversee the remediation of all risk(s) that has remediation plans developed as stated in the table above.

# risk remediation in progress #

Responsible Party

Date

Security Review Process in Human Subject Research Studies

- How to request an OIT Security Review

- Our ServiceNow
  Request Form direct link:
  - https://emory.service-now.com/sp?id=sc_cat_item&sys_id=13b886852b70f100427d2ca119da1536

- Our ServiceNow Request Form browser navigation:
  - https://help.emory.edu
  - Click on "Request Something"
  - From the left-hand menu, click on "Security Management"
  - Center-section of the page, click on "Security Review Process Intake Document"

Topics:

Part 2 - continued

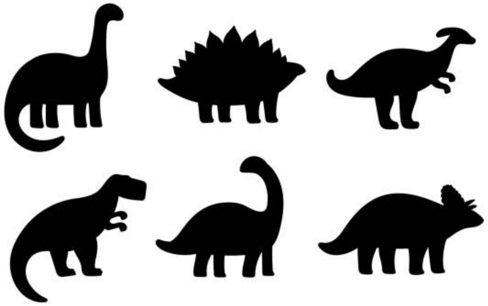
**(If the first portion of Part 2 was 2a,
is this 2b – or not 2b? This is the question.)**

New Process Improvements

New Security Process Improvements Specifically for Research Studies

- We’ve discovered a New Dinosaur
- Security’s New SharePoint Communications Site
- New / Updated OIT-Reviewed and Approved List of Applications, Tools, Solutions for Studies with Identifiable Data

We’ve Discovered a New Dinosaur



- Our New Dinosaur:
  - The DINASR
  - “Do I Need A Security Review”
- Microsoft Forms based self-service tool to help research study teams determine if they need a security review
- An interactive Q&A format that branches into various subject areas depending on responses
- Will be published soon on our new SharePoint communications site (available to all Emory personnel)

Short Demo:
New Security Process Improvements

- Information Security Architecture Team's New SharePoint Communications Site

- New / Updated OIT-Reviewed and Approved List of Applications, Tools, Solutions for Studies with Identifiable Data

Some Additional Security Review Process Improvements Topics Which Are In-Flight

- AI solutions / Emory's AI Security Policy
- Wearables
- Transcription Services
- Continuing to Update the OIT-Reviewed and Approved List of Applications, Tools, Solutions for Studies with Identifiable Data