SCORE Meeting

May 11, 2017

Presenter: Zachary Arnold,

Privacy Officer for Research and Academics

Privacy Safeguards

Administrative

- Policies, procedures, training
- Appointment of privacy officers

Technical

- Control of access to information - passwords
- Establish audit controls, checks
- Verifying identity of persons seeking access to PHI
- Encryption of PHI

Physical

- Control of access to facilities and areas
- Ensuring proper use/location of workstations
- Protection of devices/media

Most Common Privacy Issues

Inappropriate Disclosure via …

Email and Fax

Social Media

Inappropriate Use …

Access to records for non-job related reasons

E-mail Communication

HIPAA Policy 0P29 Electronic Transfer of PHI via Facsimile, Electronic Medical Record and E-mail

E-mail consent form required (for research as well as treatment) in advance of e-mailing subject - Acknowledges risks/limitations of using e-mail

- Customized research e-mail consent form on RSRB site (http://www.rochester.edu/ohsp/rsrb/docTemplates/consentFormTemplates.html)
- Use blind copy line when sending to multiple recipients
- Include a confidentiality notice
- Double check email address

Research Subject E-mail Consent Form

Subject name: _____
Subject #: _____
Subject e-mail: _____
Researcher: _____
Researcher e-mail: _____
Authorized representative:
Name: _____
Relationship: _____
E-Mail: _____

1. RISK OF USING E-MAIL

Transmitting subject information by e-mail has a number of risks that subjects should consider. These include, but are not limited to, the following:

a) E-mail can be circulated, forwarded, stored electronically and on paper, and broadcast to unintended recipients.
b) E-mail senders can easily misaddress an e-mail.
c) Backup copies of e-mail may exist even after the sender or the recipient has deleted his or her copy.
d) Employers and on-line services have a right to inspect e-mail transmitted through their systems.
e) E-mail can be intercepted, altered, forwarded, or used without authorization or detection.
f) E-mail can be used to introduce viruses into computer systems.

2. CONDITIONS FOR THE USE OF E-MAIL

The researcher cannot guarantee but will use reasonable means to maintain security and confidentiality of e-mail information sent and received. The subject and researcher must consent to the following conditions:

a) E-mail is not appropriate for urgent or emergency situations. The researcher cannot guarantee that any particular e-mail will be read and responded to.
b) E-mail must be concise. The subject should schedule an appointment if the issue is too complex or sensitive to discuss via e-mail.
c) E-mail communications between subject and researcher will be filed in the subject's research record.
d) The subject's messages may also be delegated to any member of the study team for response.
e) The researcher will not forward subject-identifiable e-mails outside of URMC and Affiliates without the subject's prior written consent, except as authorized or required by law.
f) The subject should not use e-mail for communication regarding sensitive medical information.
g) It is the subject's responsibility to follow up and/or schedule an appointment if warranted.
h) Recommended uses of subject-to-researcher e-mail should be limited to:
    a. Appointment requests
    b. Prescription refills
    c. Requests for information
    d. Updates to information or exchange of non-critical information such as laboratory values.

3. INSTRUCTIONS

To communicate by e-mail, the subject shall:

a) Avoid use of his/her employer's computer.
b) Put the subject's name in the body of the e-mail.
c) Put the topic (e.g., study question) in the subject line.
d) Inform the researcher of changes in the subject's e-mail address.
e) Take precautions to preserve the confidentiality of e-mail.
f) Contact the researcher's office via conventional communication methods (phone, fax, etc.) if the subject does not receive a reply within a reasonable period of time.

4. SUBJECT ACKNOWLEDGMENT AND AGREEMENT

I acknowledge that I have read and fully understand this consent form. I understand the risks associated with the communication of e-mail between the researcher and me. I consent to the conditions and instructions outlined here, as well as any other instructions that the researcher may impose to communicate with me by e-mail. I agree to use only the pre-designated e-mail address specified above. Any questions I may have had were answered.

_____
Subject or Authorized Representative signature

Date _____

_____
Researcher signature

When is e-mail consent required?

- Required
  - To communicate with enrolled subjects regardless of whether there is PHI in the e-mail
  - Review risks, conditions, instructions with subject and obtain signature
  - If known at time of study, design that e-mail communication will be a requirement of participation, include information in consent/authorization (separate e-mail consent form not required)

- Not required
  - Prior to enrollment *if* potential subject has provided an e-mail address to you for purposes of research recruitment

Easy, right?

Let’s see…

Example 1

Q: Jen is a Research Associate who obtained an email from a database of individuals who are interested in participating in research. She sends an email to the individuals that explains they may be eligible to participate in a research study on HIV, based on their diagnosis.

Are Jen's actions appropriate?

A: No. While the Privacy Rule allows for researchers to utilize PHI for recruitment purposes (i.e. for identification of potential subjects),the rule requires that we make an individual aware of the potential dangers of email communication if we include PHI. University policy fulfills this requirement by requiring we have email consent on file before we email PHI. Jen's email includes specific PHI about the potential subjects (diagnosis). Jen would need to have an email consent from the subject in order to communicate specific details of the study with the subject.

So, what's the solution?

Minimum necessary…

Jen can send a generic email to the patient to let them know they may be eligible for a study and provide a contact phone number for the patient to contact if they are interested in enrollment.

After the patient is enrolled in the study, Jen can communicate with the patient ONLY after they have signed an email consent form AND the IRB approved protocol includes email as a method of communication.

Example 2

Q: Study Coordinator S wishes to send an e-mail containing PHI to another colleague out-of-state. He plans to use his non-URMC and Affiliates personal e-mail account.

Is this acceptable?

A: No. Assuming that Coordinator S has permission to share the information with the colleague (e.g. as defined in the study protocol with a supporting waiver of consent or valid authorization), he should be sending the email from his UR account with !secure in the subject line).

So, what's the solution?

Minimum necessary…

A few conditions need to be met:

1. Sharing of the information for research purposes needs to be appropriate (i.e., either with authorization from the patient or waiver of consent issued by the IRB).

2. The method of sharing the PHI (emailing in this instance) needs to be approved (i.e., outlined in the study protocol).

3. Emailing PHI requires that the email be encrypted.

Example 3

Q: Mike is a study coordinator. He had previously reached out to a potential human subject via email to determine the person's interest in participating in research. Using email to communicate with the patient is not in the protocol, and as such, the human subject has not signed an email consent. Since then the patient has been consented to participate in the study and emails Mike about the results of his last procedure.

Can Mike respond to the patients email?

A: That depends. Mike may respond to inform the patient that they need to sign an email consent in order to continue the conversation. Mike should also amend the protocol if utilizing email wasn't initially described as a method of communication.

Example 4

Q: If I send an e-mail with no PHI that has a link to a web-based questionnaire do I need to encrypt it?

A: If the study questionnaire relates to a specific health condition or would allow someone other than the subject reading it to know that the subject is in a research study it should be encrypted.

Secure E-mail

When in doubt, use !Secure

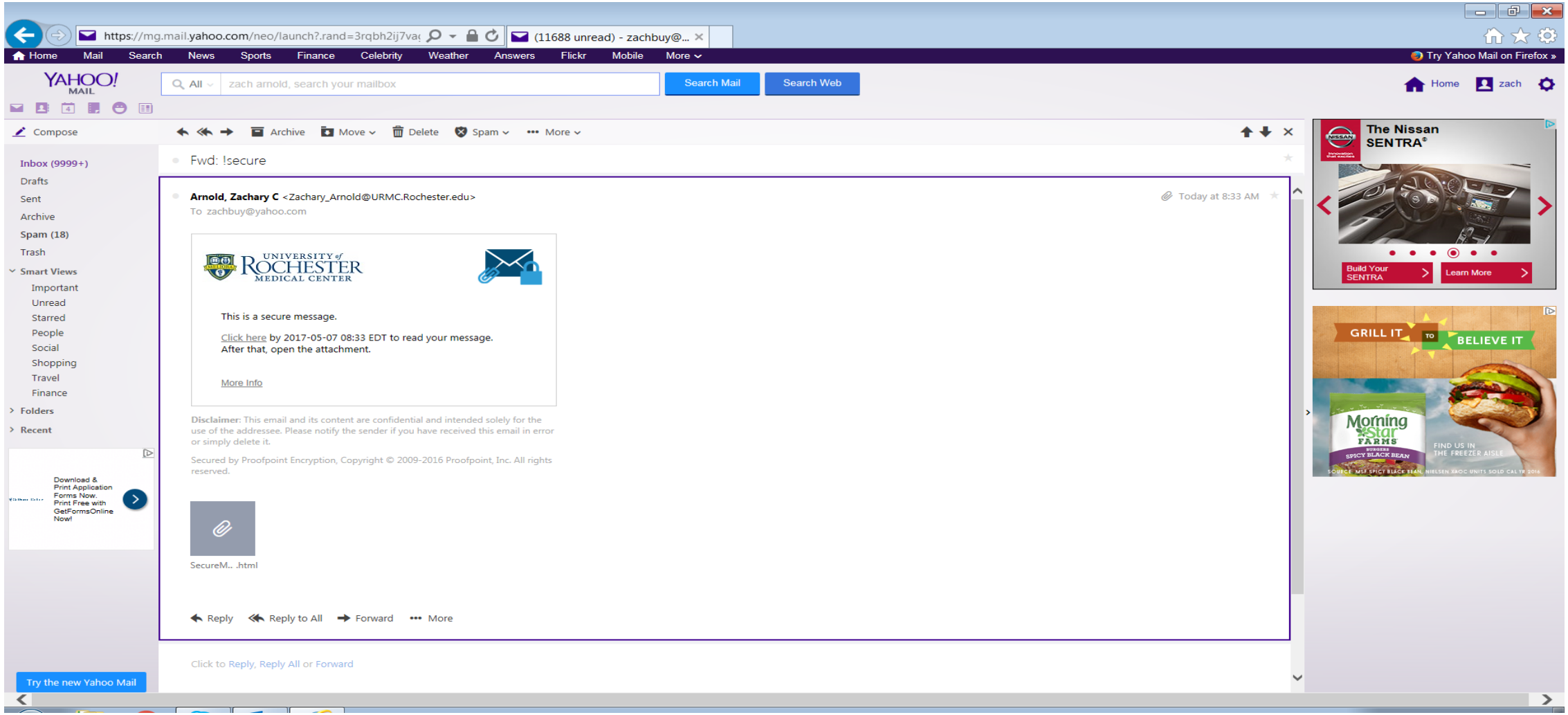
Secure (encrypted) E-mail Service

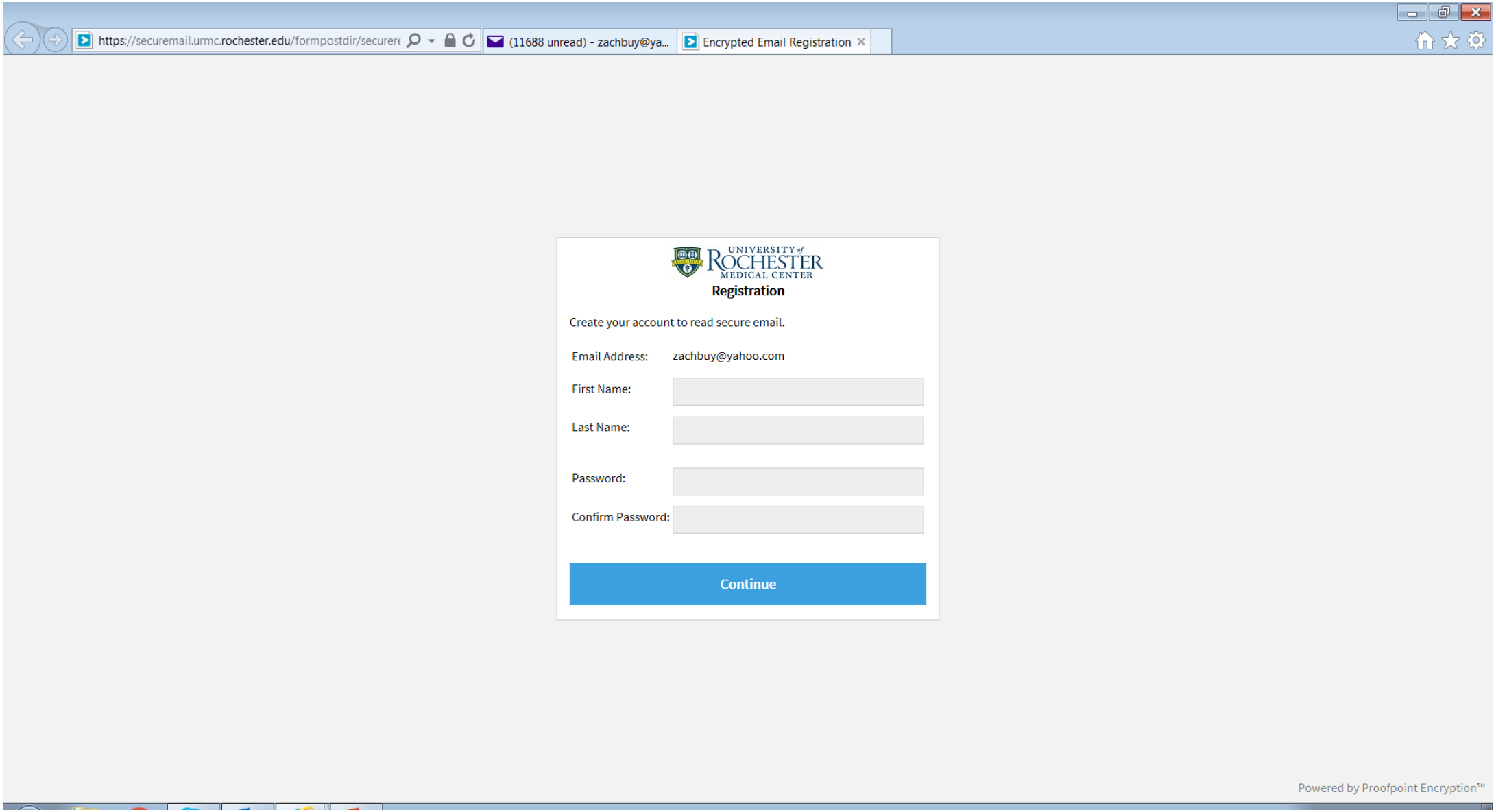
- Required when PHI is transmitted
- Must notify recipient in advance so will know to set up password
- Type **!Secure** anywhere in subject line
- If e-mail is misdirected/intercepted it will not be a privacy breach if encrypted
- Use secure e-mail when communicating with sponsors, other sites, etc.

Exception – Secure Community Partners

- Secure messaging is in place with certain area health systems, health plans, Monroe County, RHIO and others
- See list on ISD website at https://sites.mc.rochester.edu/information-systems/get-help/email/secure-email-service.aspx

What it looks like…




https://securemail.urmc.rochester.edu/formpostdir/securere
(11688 unread) - zachbuy@ya...
Encrypted Email Registration
UNIVERSITY of ROCHESTER MEDICAL CENTER
Registration
Create your account to read secure email.
Email Address: zachbuy@yahoo.com
First Name:
Last Name:
Password:
Confirm Password:
Continue
Powered by Proofpoint Encryption™

Texting PHI

It is not acceptable to send PHI through SMS (Short Message Service) Text Messaging (standard service available on mobile phones).

SMS can still be very useful. It is recommended to format text messages in a manner that provides clinical relevance in the absence of PHI. Below is an example of an acceptable text message:

"Dr. Smith, this is Dr. Jones. I just performed a lap chole on your patient JP. Everything went well. Please feel free to call with questions."

This message identifies the sender, the patient is in context, and an easy method for follow up is created. Note, however, there is no patient-identifiable information in this message. A full list of identifiers can be found in URMC and Affiliates Privacy Policy 0P30.

Using an electronic device? Encrypt it.

- Remember, SMS (basic text messaging) PHI is not allowed, even with on an encrypted device.
- Remember, if it stores URMC and Affiliates PHI or sensitive data, it must be encrypted! Never store PHI on an unencrypted device. EVER.

How do I encrypt my device?

- On most devices, such as smartphones and tablets, when you connect to the URMC e-mail, you will be forced to encrypt your device (not true for connecting to Web Mail).
- For devices other than smartphones and tablets, help encrypting your device is available by contacting your IT Support or the Information Security Office at InfoSec@urmc.rochester.edu.

Email consent combined with informed consent?

Yes!

If your study will leverage email to communicate with Human Subjects, you can consider using the RSRB template that combines the HIPAA compliant authorization and email consent with the informed consent.

Consent templates are on the OHSP page, here:

https://www.rochester.edu/ohsp/rsrb/docTemplates/consentFormTemplates.html

Resources

HIPAA website on URMC intranet:

https://sites.mc.rochester.edu/departments/hipaa/

- Policy Manual (0P25 Use or Disclosure of PHI for Research Activities)
- HIPAA Highlights
- Frequently Asked Questions – Privacy and Security
- Summary of Research Procedures, Guidelines, Forms

Resources, continued

- Research Subjects Review Board: http://www.rochester.edu/rsrb/
- Office of Human Subject Protection: https://www.rochester.edu/ohsp/index.html
- Department of Health and Human Services – Understanding the HIPAA Privacy Rule: http://privacyruleandresearch.nih.gov/pr_02.asp
- Privacy and security officers