AAHRPP
Association for the Accreditation of Human Research Protection Programs, Inc.®

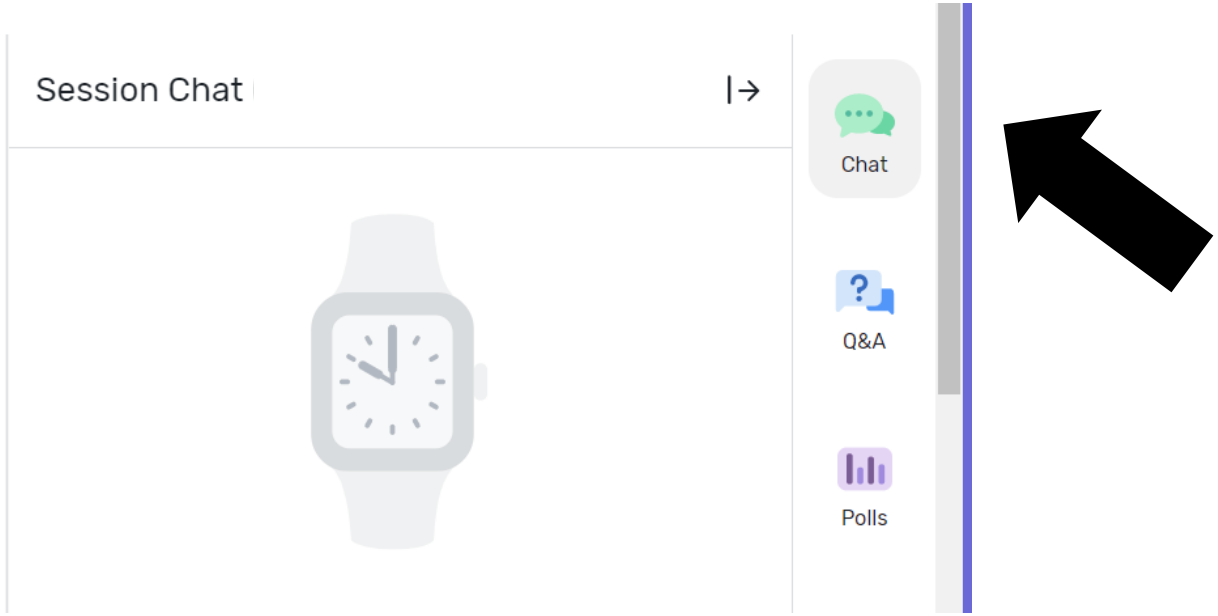
2026 AAHRPP Webinar Series

Cybersecurity and Research Data Protection: What Every HRPP Should Know

November 10, 2026: 1:00 pm – 2:30 pm ET

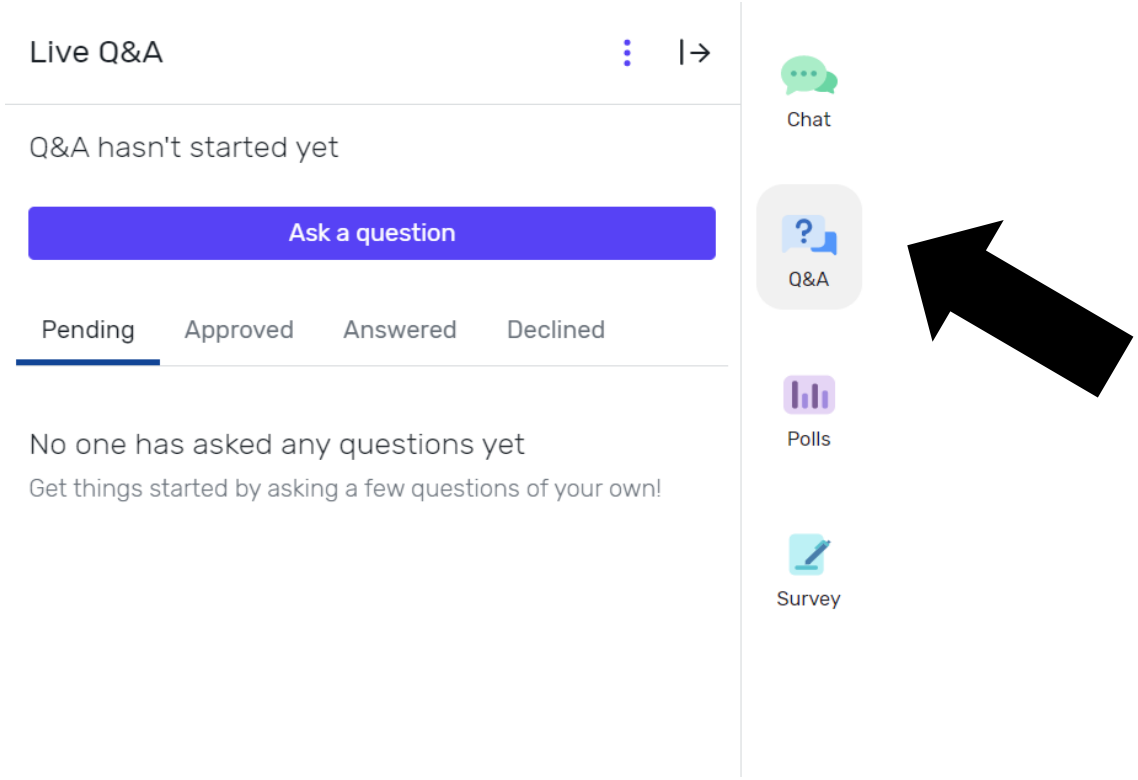
Chat Feature

To chat with your colleagues before and after the session, or if you have technical questions, use the “Chat” icon



Questions

To ask questions about the topic for the presenters, please use the “Q&A” icon:



AAHRPP
Association for the Accreditation of Human Research Protection Programs, Inc.®

Upcoming Webinars

Ask... AAHRPP

Save the following date for the last webinar of the 2026 "Ask AAHRPP" webinar series:

Tuesday, December 8, 2026, 3:00pm ET:

Responding to Council Review and Maintaining Accreditation

Visit Webinars (aahrpp.org) for more information and registration links



2027 AAHRPP ANNUAL CONFERENCE

Accreditation and Ethics in Atlanta: Turning Process into Progress

MAY 25-27, 2027 **Atlanta, Georgia**

MARK YOUR CALENDARS FOR ONE OF THE RESEARCH COMMUNITY'S MUST-ATTEND ANNUAL EVENTS. MORE DETAILS TO FOLLOW.

Visit AAHRPP's Annual Conference page for more information

Claim Your 1.5 CIP Credits

After the webinar, we'll send you a link to the Attendee Hub



Visit the Attendee Hub



View the Slides and Recording



Complete the Survey and get Link to Certificate of Attendance



Download Your Certificate of Attendance

AAHRPP

Association for the Accreditation
of Human Research Protection Programs, Inc.®

Presenter Introductions



AAHRPP

Association for the Accreditation
of Human Research Protection Programs, Inc.®



Tonya Ferraro
AAHRPP



Joseph (Joe) Zurba

Harvard Medical School



Andrea Collins

UConn and UConn Health



Kimberley (Kim) Serpico

The Broad Institute

Where does cybersecurity show up within the AAHRPP standards and elements?



Where does cybersecurity show up within the AAHRPP standards and elements?



Cybersecurity is a Shared HRPP Responsibility



What can responsibility look like across the HRPP?



IT and information security: Systems, access controls, vendors, security incidents

IRB: Risk assessment, consent, confidentiality protections, ongoing oversight…

Privacy and compliance: Data use, legal requirements, breach assessment, reporting

Researchers and study teams: Data collection, storage, sharing, security practices

How can HRPPs protect participants against cybersecurity risks when responsibility is shared across the HRPP?



AAHRPP
Association for the Accreditation of Human Research Protection Programs, Inc.®

2026 AAHRPP Webinar Series

Cybersecurity and Research Data Protection in Human Research

Joseph Zurba, CISSP, CISA
Director of Research Security & Regulatory Compliance
Harvard Medical School, Information Technology

Disclosure Statement

I have no relevant personal/professional/financial relationship(s) with respect to this educational activity

Joseph Zurba, CISSP, CISA

Cybersecurity is simple, right?

Turns out…no

- Constantly evolving tech landscape
- Tech moves faster than most organizations can keep up with
- Democratization makes new tech available to researchers who are anxious to use it…with or without permission
- Vulnerability and certificate management are becoming an ongoing nightmare

Vetting tools and services

- Good resources include:
  - FedRAMP marketplace (fedramp.gov/marketplace)
  - GovRAMP (formerly StateRAMP) (govramp.org)
  - CISA (Cybersecurity and Infrastructure Security Agency) (CISA.gov) Provides no-cost cybersecurity services and tools
- Third-party assessment documents
  - SOC 2 (Security and Organizational Controls)
  - HITRUST - for health information
  - SAR (Security Assessment Report)

Caveats

There are no magic bullets



Cloud Service Providers

- Avoid the myth that just because your CSP is compliant, so is the project
- Think of the cloud as “servers in Virginia” and assess accordingly
- Compute is still very expensive – computationally intensive projects should still be done on-premises



I’m using AWS, and AWS is compliant

I have a SOC2 from my data center provider

I’m setting up my own server

I’m using a new online service or tool



How long will I keep my data?

What's the data life cycle?

The AI Slide

- AI can be very useful if used with the right safeguards
  - Contract that protects the institution and its data
    - Provision that institutional data is not used to train its model(s)
    - Data security and privacy language
    - User-provided data is separate
    - Destruction language
  - For sensitive data, consider using a local LLM

Engage with your IT department (if you can)

- Don’t try to develop expertise within your IRB
- Don’t trust researchers to do their own tech
- IT Departments should invest in the tools that researcher want/need (hint – it’s not Microsoft)

AAHRPP
Association for the Accreditation of Human Research Protection Programs, Inc.®

2026 AAHRPP Webinar Series

Cybersecurity and Research Data Protection: What Every HRPP Should Know

Andrea Collins, MHA, CIP
UConn and UConn Health

Disclosure Statement

I have no relevant personal/professional/financial relationship(s) with respect to this educational activity


Sponsored Programs
IRB
Information Security Office
UConn and UConn Health
FERPA Privacy Office
Records Management Office
Office of Healthcare Compliance & Privacy

Data Security Assessment Form

- Section A: Information to be used or collected for the research
- Section B: Collection of research data
- Section C: Transmission, processing, and storage of research data
- Section D: Data management
- Section E: Artificial Intelligence (AI)
- Section F: Other information regarding confidentiality risks and risk mitigation that you believe may be important for the IRB's review

➢The form depends on investigators providing accurate information

Section A: Information to be used or collected for research

- Data elements
- Geolocation data
- Sensitive information
- FERPA data

Section B: Collection of research data

- Mobile App
  - Is the app being used as intended and consistent with the terms of service?
  - What device(s) will be used to access the app?
  - Will personal data be stored on the devices for any interval of time?
  - Will the app be able to access other device functionality, such as Location, Contacts, Notifications, Microphone, etc.?

Section B Continued

- Text messaging
- Survey platforms
- Software
- Audio or video recording, video conferencing, or photographic images
  - ➢ Connecticut has state laws regarding recording and consent that must be taken into consideration
  - ➢ Other states/jurisdictions may also have laws or requirements that may need to be taken into consideration

Section C: Transmission, processing, and storage of research data

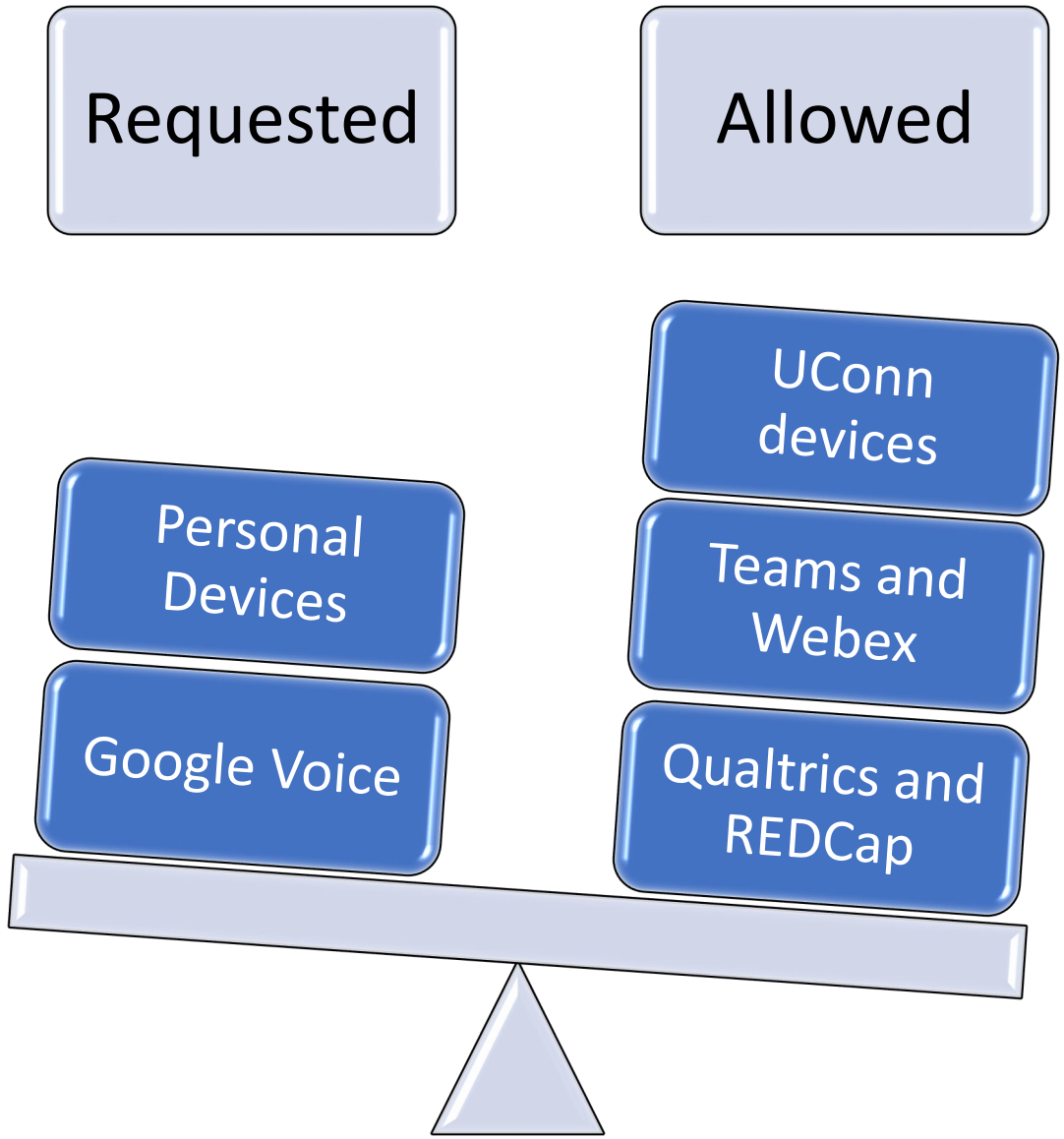
- Describe where/how the transmission, processing, and storage of data will take place for all aspects of the research

Section D: Data Management

- Who will have access to research data and records?
- Describe how access will be managed?
- How long will research data/records be maintained?
- Will data or specimens be transferred to a repository?

Section E – Artificial Intelligence (AI)

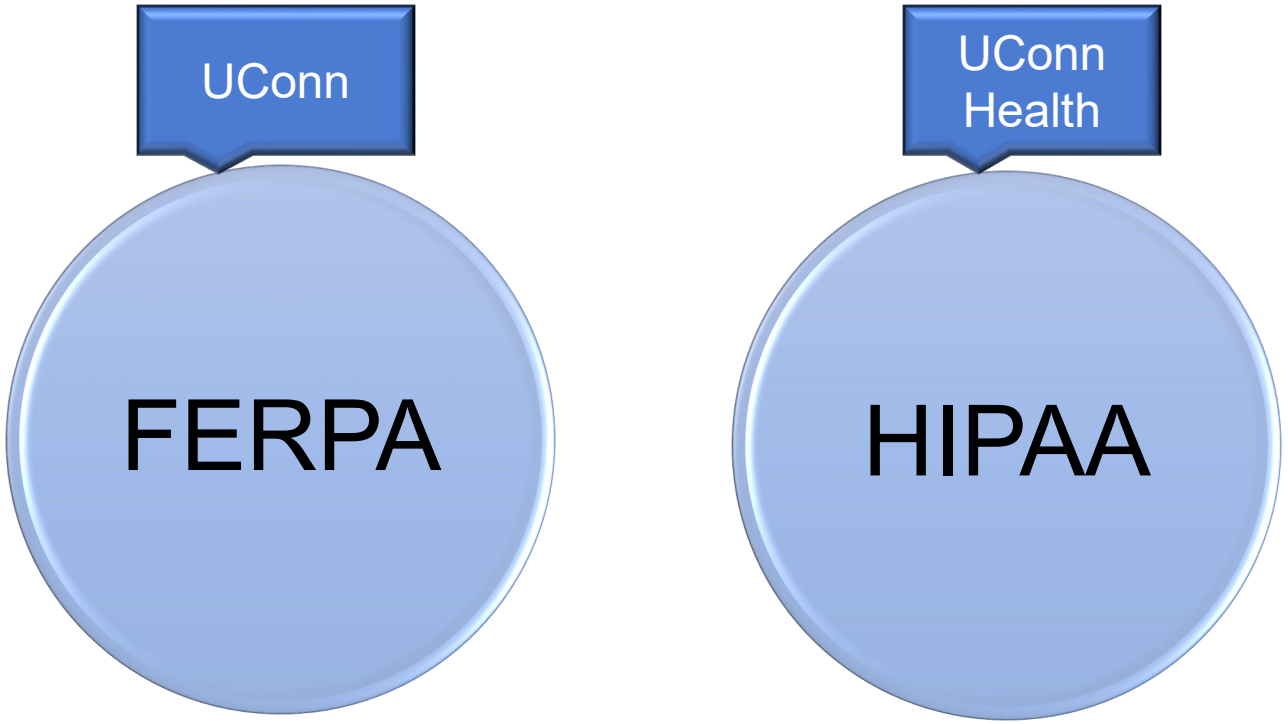
- Is the study using established AI?
- Developing AI or training, validating, or testing?
- Evaluating AI?
- Specify the type of data AI will have access to (Protected, Sensitive, Identifiable)


Requested
Allowed
UConn devices
Personal Devices
Teams and Webex
Google Voice
Qualtrics and REDCap

Consent Considerations

- Include information regarding any terms of service or end user agreements that participants must agree to prior to participation in research
- Include a risk statement about the use of third-party software
- Specify the management of participant information
- If participant data will be processed by AI, this should be disclosed in the consent materials
- When a publicly available privacy statement, terms of use, or other documentation addressing confidentiality and data use exists, a link should be provided

Regulations That Impact Data Protection



• The Family Educational Rights and Privacy Act (FERPA)

A federal law that protects the privacy of student education records

- FERPA requires written consent from each student prior to the disclosure of personally identifiable information (PII) within education records, with limited exception
  - ➢ The IRB does not have the authority to waive any part of this requirement

Risks: Email – FERPA

- UConn has not designated email addresses as “Directory Information,” which means they cannot be shared with researchers for recruitment purposes
- Researchers may not directly access or use departmental or program student email lists to send recruitment materials for study participation

Risks: Email – HIPAA

- Do not put PHI, PII, or other confidential data in the subject line of an email

Example:

- Subject Line: *Recruiting Anxiety Clinic Therapy Patients*

Risks: Departures

- Investigators take their data
  - DUA, DTA, MTA may be required
- Encryption standards vary from country to country
- Data privacy regulations vary between states
  - Investigators are responsible for understanding the data privacy laws where data collection occurs under their protocol

Risks: Bots

- Prior to 6:29pm, 19 participants enrolled in a survey study
- Between 6:29PM and the following morning, the researchers received over 6,200 Qualtrics survey responses
- Qualtrics support confirmed that bot detection, CAPTCHA or reCAPTCHA, checks for duplicate responses, the Security Scan Monitor, and blocking of search engines were all in place



Final Thought

"When a critical vulnerability is announced, uncertainty about ownership can delay remediation efforts and increase organizational risk."

Understanding the Changing Vulnerability Landscape | IT Security | Information Technology Services | University of Connecticut

AAHRPP
Association for the Accreditation of Human Research Protection Programs, Inc.®

2026 AAHRPP Webinar Series

Cybersecurity and Research Data Protection in Human Research

Kim Serpico, EdD, CIP
Director, Research Compliance & Human Research Protections
Broad Institute (kserpico@broadinstitute.org)

Disclosure Statement

Kim Serpico - I have no relevant personal/professional/financial relationship(s) with respect to this educational activity.

An HRPP without an IRB: the Broad Institute model

My lens: An HRPP that designs, oversees, and implements data protection across many organizations and amidst multiple sIRB rules.

No IRB

The Broad HRPP protects participants without operating an IRB of its own.

Reliance

The majority of our human research is reviewed by external IRBs under reliance agreements.

Two levels of protection: Organization & IRB

Organizational Security/HRPP

- Owned by security, IT, privacy and compliance offices (HRPP)
- Network, cloud and access controls
- Vendor and tool risk assessment
- Incident response and breach notification

IRB Review

- Are privacy and confidentiality protections adequate for this study?
- Does consent describe data use and limits of confidentiality?
- Is the risk of a data compromise matched by the protections?

The IRB relies on institutional security; it does not replace it.

Reliance agreements: Where security gets negotiated

In a reliance model, these questions get answered in the agreement or not at all.

1. **Whose rules?**
   Which security standards govern the data: the reviewing IRB's, the relying institution's, or the sponsor's?

2. **Who vets the tools?**
   Who reviews platforms, vendors and storage before the study starts?

3. **What must the IRB see?**
   What security information reaches the reviewing IRB so it can make its privacy and confidentiality determinations?

4. **Who reports incidents?**
   Who is told, by whom, and how fast when a data incident affects participants?

Research activities that raise cybersecurity risk

Secondary analysis and linkage
Combined datasets can make people identifiable, even if each file looks de-identified.

Data sharing and repositories
Once data leaves our control, protection depends on someone else's safeguards.

Multi-site and international work
More institutions bring more security standards and more transfer rules.

Remote and electronic collection
Apps, surveys and wearables put data on devices we do not manage.

Sensitive data and populations
Breached genomic or behavioral-health data can cause lasting harm.

Large, rich datasets
More data per person raises the stakes of any single compromise.

Secondary research: Risk without participant contact

1 Obtain

- Does consent cover this use?
- What security terms come with the data?
- Is it identifiable or coded?

2 Analyze

- Linkage can re-identify people
- Secure environment or laptop?
- Who has access?

3 Share and retain

- Downstream sharing and repositories
- Small cells and genomic data in publications
- Retention and destruction

Practical approach: Security built into HRPP workflow

1	**Intake**	IRB submission system as the single front door and system of record for research determinations
2	**Determination**	A standardized IRB application asks the right data questions up front
3	**Data-risk triage**	Flag identifiable, coded, or sensitive data and scale review to the risk
4	**Agreements**	Align reliance agreements and data use terms with security requirements
5	**Oversight**	Track changes, incidents, and monitoring in the same record

Key Takeaways

Organizational security and IRB review are different jobs. Define both.

Negotiate data protection into every reliance agreement.

Treat secondary research as participant risk, not paperwork.

Plan for incidents before they happen: who reports what, to whom, & how.

Resources

https://catalyst.harvard.edu/publications-documents/important-it-considerations-for-irbs/

https://catalyst.harvard.edu/publications-documents/providing-it-expertise-to-the-irb/

Thank You!