UNIVERSITY *of* MARYLAND
BALTIMORE

HIPAA

Security and Privacy of Data, With a Special Focus on Research

November 3, 2022

Session Contributors

- Peter Murray, PhD, CAS, MS, Senior Vice President for Information Technology and Chief Information Officer
- Julie Doherty, DM, MSN, RN, CIP, CCEP, Assistant Vice President, Human Research Protections Program, Office of Accountability & Compliance
- Jan Martinez, MS, CIP, CLSSGB, IRB Manager, Human Research Protections Program, Office of Accountability & Compliance Research Compliance
- Gregory F. Ball, PhD, Vice President for Research for UMCP and UMB
- Irma Robins, MBA, JD, UMB Deputy General Counsel

What is HIPAA?

- HIPAA stands for the “Health Insurance Portability and Accountability Act”. It was passed by Congress in 1996.

- The U.S. Department of Human Services (HHS) published a **Privacy Rule** in December 2000 and modified it in 2002. Compliance with the Privacy Rule was required as of April 2003. HHS published the **Security Rule** in 2003. Compliance with the Security Rule was required as of April 2005.

- The **Privacy Rule** set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. The **Security Rule** set national standards for *protecting the confidentiality, integrity, and availability of electronic protected health information*.

HIPAA and Privacy and Security Rules

Why Would I Need to Know About Them?

- It is the law, and there are significant penalties for not complying with the Rules.

- Each of us has a responsibility to respect and protect the privacy and security of all personally identifiable information (PII).

- UMB professionals need to know and understand institution policies and procedures for protecting sensitive data; and take note of best practices for protecting personally identifiable information, including protected health information.

- Cyber criminals do nefarious activities and cause great harm when they obtain PII.

The Security Rule

Requires appropriate technical safeguards to ensure the security of electronic protected health information

Cyber Attacks are the #1-way health records are breached

- ➢ UMB receives approx. **1.2 billion attempts daily** to get access to systems and data;
- ➢ Approx. **500K** of these attempts are blocked because they are known security threats;
- ➢ UMB receives approx. **600K emails daily**
  - ✓ Approx. 15K emails are blocked because they are known phishing attempts;
  - ✓ Approx. 300 emails are quarantined because they contain malware.

IT Security Rules and Best Practices for Protecting PII/PHI

Passwords: Make them Strong! At UMB, the password must be a minimum must be 12 characters; The password should always be kept private and NOT shared with anyone.

Multifactor Authentication (MFA) must be used for accessing systems and confidential data; Only accept MFA requests when you are actively trying to login to a system or application.

Computers must be password protected; are using the latest version of the operating system; using software that provides anti-virus protection; and are secured by logging off or shutting down when they are not in use.

Secure Cloud-based File Storage should be used for storing sensitive information.

Public Wi-Fi must not be used unless you have implemented a VPN connection that utilizes MFA.

Text Messages that contain sensitive information should not be sent unless a secure messaging solution is being used.

Social Media, never post sensitive information could identify the protected health information of a person.

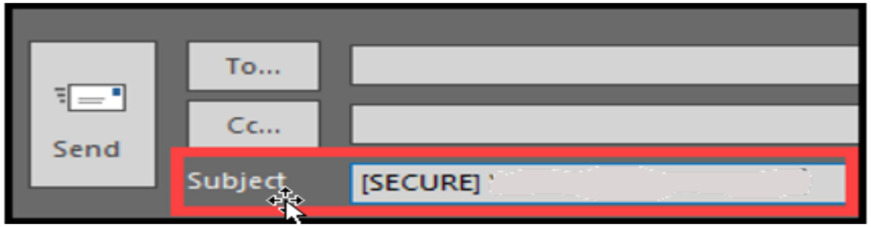
Beware of suspicious emails and phone calls as they could be phishing scams and/or contain malware. Do not open any emails from untrusted sources.

Avoid Unintentional Disclosures in E-mail

- Check e-mail address for accuracy;
- Use UMB email account for all e-mails, especially containing ePHI. Don’t use personal email accounts to send ePHI on or off campus;
- **Use a secure email solution** when sending any confidential information (PII, PHI).

Secure Method for Protecting PHI When Sending via Email

- Safeguarding ePHI sent in e-mails by encrypting it. **Type [SECURE] in the subject line:**
  - UMB faculty, staff and students have the ability to send encrypted emails by simply adding [secure] to the subject in an email;
  - When sending any confidential information (PII, PHI, credit card information, etc.), it is strongly recommended to use this method to ensure that only the recipient can view the information;
  - To encrypt an email message, add [secure] to the beginning of the subject line. Be sure to include the brackets and add a space after:



Subject: [SECURE]

Protection and Disclosure of PHI

Researchers with access to protected health data may use or disclose only on a “need to know” basis:

- Keep health data secured and confidential.
- Access or use PII/PHI only as required to undertake your research.
- **Do not discuss** health information with others unless it is administratively, clinically, or **research necessary**, or a patient authorized to do so.
- DO HIPAA RULES APPLY WHEN I WORK OFF-CAMPUS?
  - **Yes**. Regardless of location, you must protect the security and privacy of PHI. When working or doing research from home, the same HIPAA rules and requirements apply, and necessary IT security precautions need to be taken (anti-virus, software updates, password-protected screen saver, etc.) on your home computer as is on your UMB office computer.

Consequences of Not Complying with HIPAA Rules

- Inappropriate disclosure of confidential information and failure to follow policies may lead to disciplinary action including termination;

- There are civil and criminal penalties for violations of patient privacy;

- There are negative impacts to an institution's reputation and ability to do future business with companies and the federal government to obtain research grants.

HIPAA Violations & Penalties

- **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided. Penalty could range from $100 to $50,000 per incident.
- **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. Penalty ranges from $1,000 to $50,000 per incident.
- **Tier 3:** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, and an attempt has been made to correct the violation. Penalty ranges from $10,000 to $50,000 per incident.
- **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation. Penalty is $50,000 and above per incident.

Sample Penalties Imposed in HIPAA Violation Cases

- ➢ These are just a small number of examples where Criminal Complaints were filed, HIPAA violations found, and penalties imposed:

- ✓ A Nurse Assistant was fired for sharing videos and photos of a patient with Alzheimer's on Snapchat and was sentenced to **3 years in jail**.
- ✓ An Insurance Carrier was **fined $2M** for placing a lack of importance of implementing safeguards for ePHI.
- ✓ A Colorado hospital failed to terminate a former employee's access to ePHI and was **fined $200,000.**
- ✓ A Company went out of business and was still **fined $3M** for HIPAA violations; consequences of HIPAA violations do not stop when a business closes.

HIPAA

Health and Human Services (HHS), and the Federal Drug Administration (FDA)

- HIPAA - Protects the data
  - Rules to protect the privacy and confidentiality of the individually identifiable health information (IIHI) that is used or disclosed by a covered entity.
- HHS and FDA - Protects the people
  - Rules to protect the rights and welfare of human participants in research studies.

Human Subjects Research and the HIPAA Privacy Rule

- An Institutional Review Board (IRB) may waive patient authorization for access PHI for certain research activities.
- Use or disclosure of PHI is prohibited unless it is authorized by the patient, permitted by law or granted through an IRB waiver.
- HIPAA insists that researchers get patient authorization and IRB approval before using or disclosing PHI.
- Under the Common Rule (Federal Policy for the Protection of Human Subjects), IRBs can exempt certain research activities that uses PHI.

.https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/common-rule-subpart-a-46104/index.html

HIPAA Privacy Rule and Research

The HIPAA Privacy Rule includes the conditions under which PHI may obtained, used and disclosed for research purposes.

- Preparatory Research (45 CFR 164.512(i)(1)(ii))
- Limited Data Sets with a Data Use Agreement (45 CFR 164.514(e))
- Research Use/Disclosure With Individual Authorization (45 CFR 164.508)

Electronic Signatures and HIPAA Authorizations

- Electronic signatures are allowed and acceptable provided they are compliant with the Federal Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA).

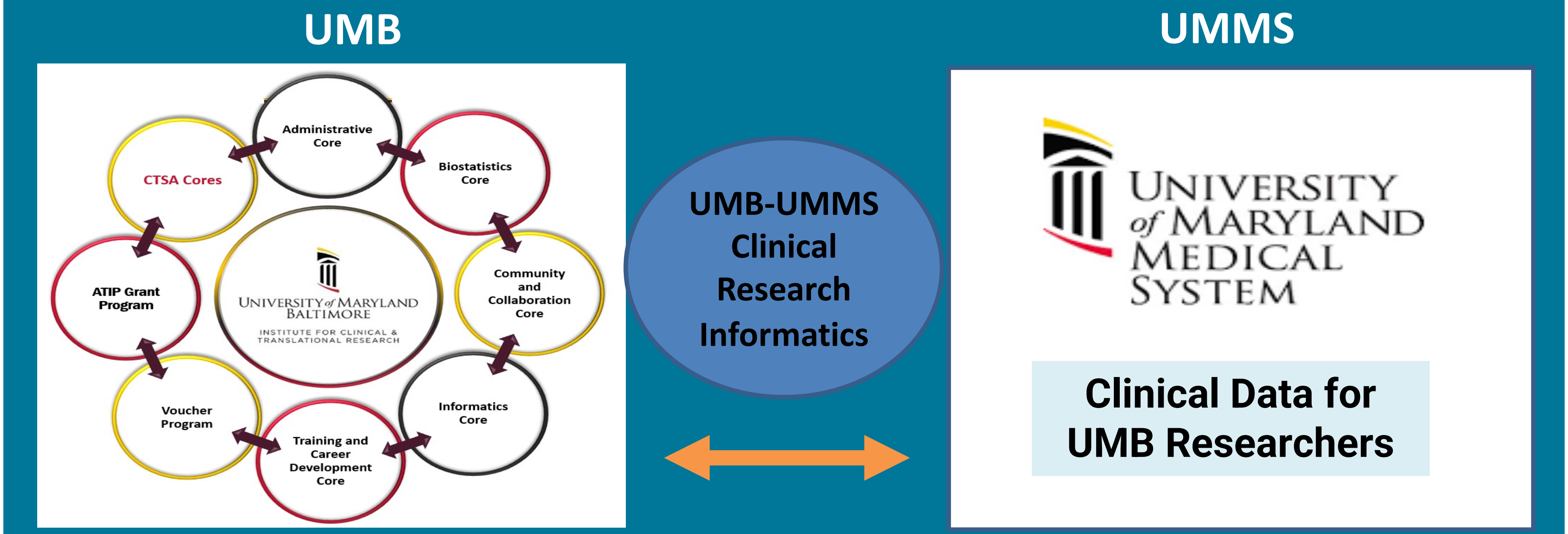
- The conditions of UETA and the ESIGN Act are: Legal Compliance; User Authentication; Message Integrity; Non-Repudiation; and Ownership and Control.

- UMB uses **DocuSign,** which is compliant with UETA and the ESIGN Act, and is therefore an acceptable and approved electronic signature solution for HIPAA authorizations.

UNIVERSITY *of* MARYLAND
BALTIMORE

UMB/UMMS Research Informatics Core and Data Use Agreement

- In 2021 UMMS and UMB jointly founded a Research Informatics Core.
- It operates with input and shared governance with the UMB ICTR.
- In 2022, UMMS and UMB created a Data Use Agreement.
- It streamlines the provision of clinical data to researchers.
- It provide expertise in extraction, transformation, harmonization of EMR and other data.



UMB

Administrative Core
Biostatistics Core
CTSA Cores
Community and Collaboration Core
ATIP Grant Program
UNIVERSITY of MARYLAND BALTIMORE
INSTITUTE FOR CLINICAL & TRANSLATIONAL RESEARCH
Informatics Core
Voucher Program
Training and Career Development Core
UNIVERSITY of MARYLAND MEDICAL SYSTEM

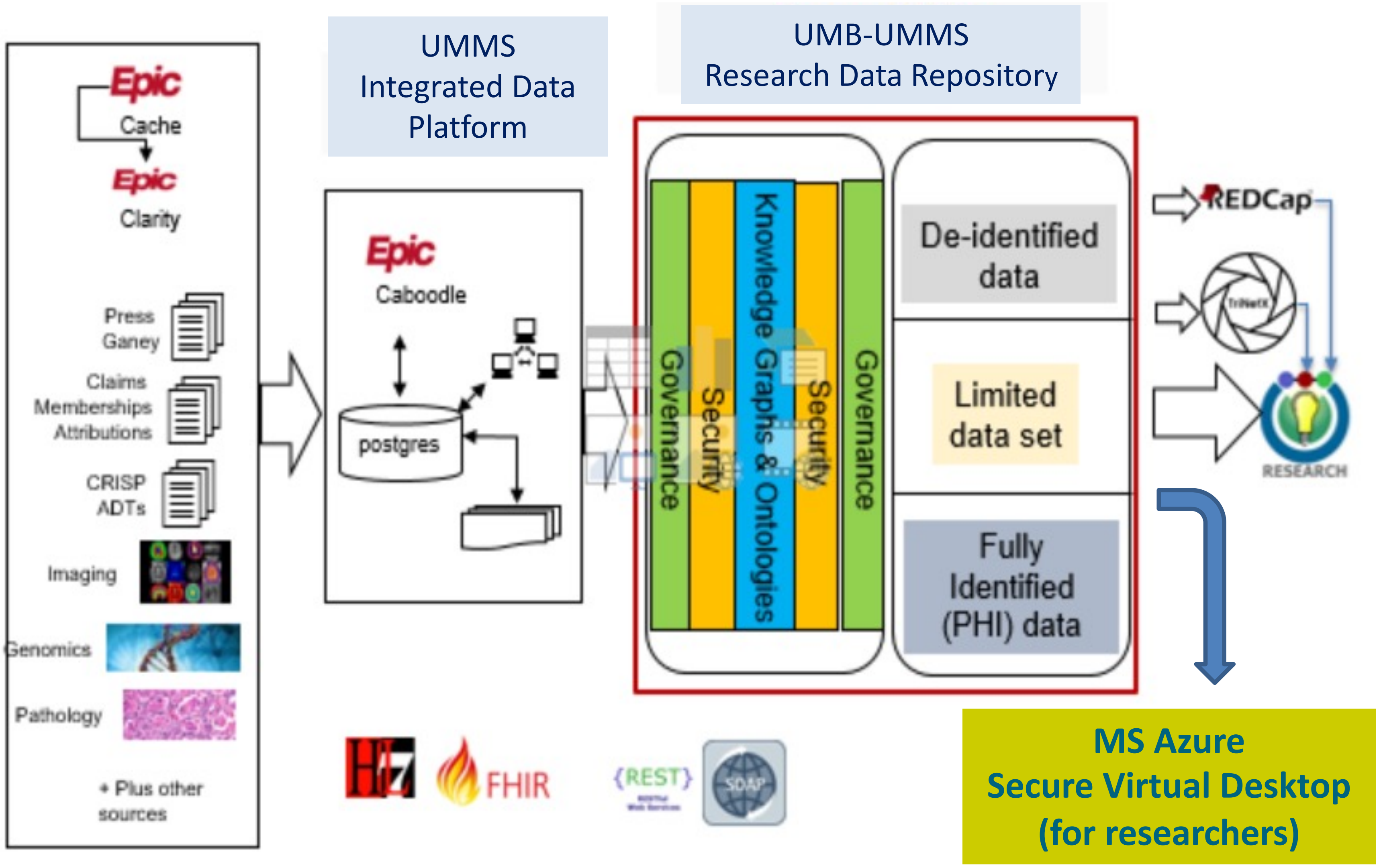
UMB-UMMS Clinical Research Informatics

UMMS

Clinical Data for UMB Researchers

UNIVERSITY *of* MARYLAND
BALTIMORE

UMB/UMMS Research Data Ecosystem



UMMS
Integrated Data
Platform

UMB-UMMS
Research Data Repository

MS Azure
Secure Virtual Desktop
(for researchers)

Secure Microsoft Azure Virtual Desktop

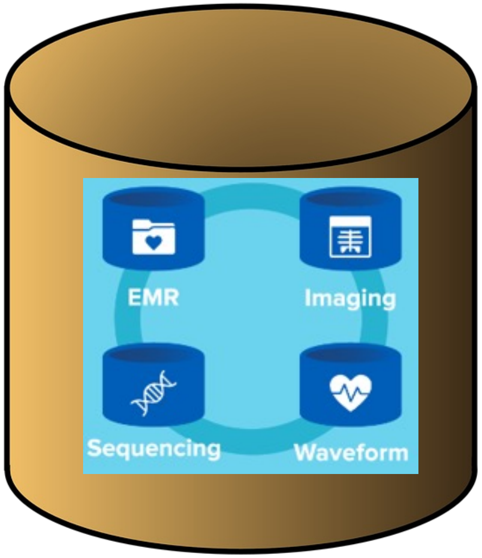
Cloud-based access

- Authorization
- Authentication
- Confidentiality
- Availability
- Integrity

Analysis

- Excel
- SAS, Stata
- R

Data



Honest Broker Services

- Patient matching
- Cataloging
- Harmonization
- Linkages and Enrichment
- Provisioning

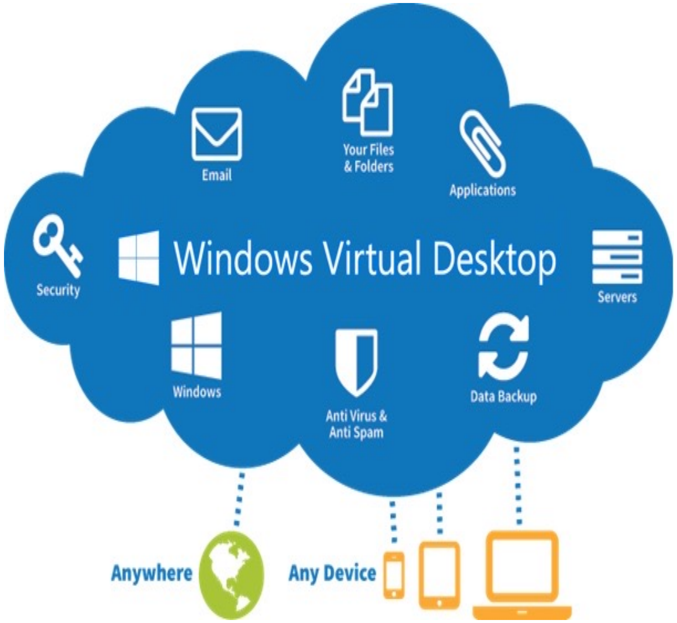
Soft launch (for pilot researchers) ~ Nov. 2022

Azure/Windows Virtual Desktop

Benefits:

- Can quickly create and deploy AVD accounts
- Efficient management of demand; can scale the use of AVD as needed
- There is a reduction in physical server hardware and hardware maintenance costs
- No need to use costly, high-end computers
- Supports multiple computing endpoints: Windows, Apple, Chromebook and Android
- Persistent Experience, access anytime and from anywhere
- Secure access to data stored in highly secured computing environments.

Enhancing Security:
A virtual desktop infrastructure
to achieve greater security



AVD for Faculty and Staff

General Use Faculty & Staff

- Access to software based on user's needs
- Deploy in minutes
- Manage demand – scale as needed
- Secure access to data

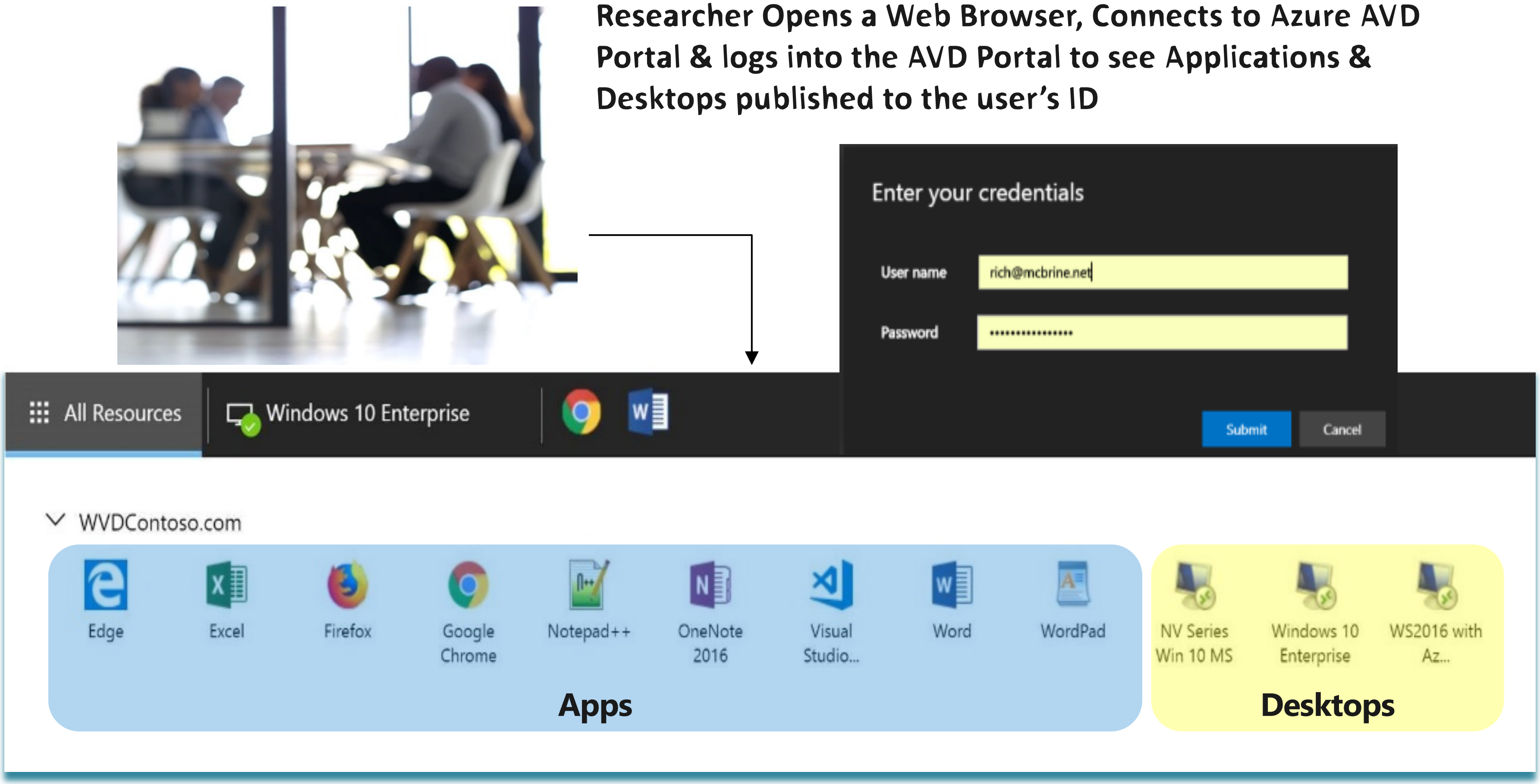
Specific Use Research

- Secure access to specific environments
- Standard Research Tools & Software Packages
- Compliance with HIPAA and other Data Security Standards
- Mitigates Risk to Personally Identifiable Information and Protected Health Data

University of Maryland Baltimore

How Do Researchers Use Azure Virtual Desktop (AVD)?

Researcher Opens a Web Browser, Connects to Azure AVD Portal & logs into the AVD Portal to see Applications & Desktops published to the user's ID



Enter your credentials

User name: rich@mcbrine.net

Password: ••••••••••••••••

New State Privacy Law

Md. Code, State Gov't § 10-13A-01

Takes effect October 1, 2024

- Changes the definition of PII – “Any information that, taken alone or in combination with other information enables the identification of an individual”.
- Allows individuals to request, modify, delete PII – so long as the University doesn’t have legitimate purpose to maintain the data.
- A privacy notice must be published and made directly accessible from the University Web homepage and on any of the webpages of the institution that are used to collect personally identifiable information.
- Requires the adoption of a Privacy Governance Program.

Important Exclusions

- It **DOES NOT** apply to personally identifiable information that:
  - **Is disclosed in accordance with the federal Health Insurance Portability and Accountability Act;**
  - **Is information related to Sponsored Research.**

New National Security Presidential Memorandum 33 (NSPM-33)

NSPM-33 Goals

- To protect America’s national security while promoting openness in the research community.

- To have clear regulatory requirements so that researchers can easily and properly comply with those requirements.

- To ensure that policies and requirements do not promote fear, xenophobia, or other forms of prejudice.

New National Security Presidential Memorandum 33 (NSPM-33)

Stated Concerns:

- Licit and illicit means of gaining access to US research technology.
- US scientists conducting secret research programs for foreign governments that require them to disclose non-public research results.
- Researchers with undisclosed outside activities that may interfere with research objectivity.
- Institutions with undisclosed foreign funding sources.
- The US commitment to “open research” and international inclusivity is not reciprocated by certain foreign governments

New National Security Presidential Memorandum 33 (NSPM-33)

Key Elements: For Agencies

- Clear and consistent guidance and policies.
- Harmonize disclosure requirements ("to the greatest extent possible").
- Allow for individuals and institutions to make corrections to previously submitted information.
- Enforce!
- Sharing of non-compliance information between agencies
- Incorporate digitally persistent identifiers into their systems and processes.

New National Security Presidential Memorandum 33 (NSPM-33)

Key Elements: For Institutions >$50M

- Written research security program subject to audit.
- Certification and oversight by a designated official.
- Robust COI program and proposal disclosure oversight.
- Enhanced cybersecurity controls.
- Export control program.
- Insider threat and export control training.
- Travel security program.

New National Security Presidential Memorandum 33 (NSPM-33)

Disclosure Requirements

NSPM-33 requires all federal research funding agencies to strengthen and standardize disclosure requirements for federally-funded awards.

- Researchers must fully, accurately, and uniformly disclose conflicts of interest and conflicts of commitment to federal sponsors. *This includes consulting activities, in-kind support, and research-related gifts.*
- All senior/key personnel must comply with the disclosure requirements.
- Federal agencies will share information about disclosure violations with each other.

New National Security Presidential Memorandum 33 (NSPM-33)

Research Security Requirements

NSPM-33 mandates that research institutions receiving more than $50M per year in federal funds establish and certify compliance with research security programs covering (1) cybersecurity; (2) foreign travel security; (3) research security training; and (4) export control training.

- **Cybersecurity** – NSTC has identified 14 protocols and procedures to satisfy the cybersecurity element, including cybersecurity awareness training and enhanced protection of scientific data from ransomware and other attacks.
- **Foreign Travel Security** – Institutions must have a foreign travel policy, provide foreign travel security briefings, provide pre-approval for foreign travel, assist with electronic device security, and otherwise assess, monitor, and keep records of foreign travel.

New National Security Presidential Memorandum 33 (NSPM-33)

Research Security Requirements (continued)

- **Research Security Training** – Institutions must provide mandatory periodic training and tailored training in the event of a research security incident.
- Training must include research security threat awareness and identification and insider threat training (unusual for institutions engaged in fundamental research).
- Institutions must designate a research security point of contact with a publicly accessible means to contact that individual.
- **Export Control Training** – Institutions must provide export control training for those participating in research subject to export control restrictions.

New National Security Presidential Memorandum 33 (NSPM-33)

DPI Requirement; Enforcement

- ➢ NSPM-33 requires the use of digital persistent identifiers (DPIs).
  - ✓ DPIs are intended to better track disclosures, increase security, and reduce administrative burdens.
  - ✓ Research institutions will need to be mindful of data privacy laws related to DPI use.
- ➢ NSPM-33 requires federal oversight and enforcement activity in the form of administrative actions and civil or criminal penalties.
  - ✓ Administrative actions include termination of research awards, mandatory return of research funds, and suspension and debarment against individual researchers and/or institutions.
  - ✓ Extreme cases could jeopardize the Higher Education Act (HEA) Title IV funds, which would result in the denial of federal student financial aid to students.

UMB HIPAA Training Education Resources

- ➢ The UMB Human Research Protections Office (HRPO) takes a proactive approach and works collaboratively with other research entities to provide ongoing education and training. To ensure the safe conduct of all individuals engaged in human subjects research, the following HIPAA education/training material is offered to UMB faculty researchers:
- ➢ Training courses include the following subject matter:
  - ❖ Privacy and Security Review
  - ❖ Information Technology
  - ❖ Human Research

The link below takes you directly to the HRPO website:
https://www.umaryland.edu/hrp/for-researchers/required-training/

The link below takes you directly to the HIPAA Online Training web page:
http://issomspweb.som.umaryland.edu/hipaa/quiz/index.asp

Some Relevant UMB Policies

UMB Acceptable Use Policy

- https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9901a.php

UMB IT Privacy Policy

- https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9915a.php

UMB Electronic Messaging and HIPAA Compliance

- https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9909a.php

UMB IT Guidelines on Collection of Personal Information

- https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9919a.php

UMB Policy Regarding Ownership, Management, and Sharing of Research Data

- https://www.umaryland.edu/policies-and-procedures/library/research/policies/iv-9901a.php

UMB Policy Regarding Cloud Computing for Confidential or Regulated Data

- https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9921a.php

UMB Data Classification Policy

- https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9906a.php

Thank You!

Questions?