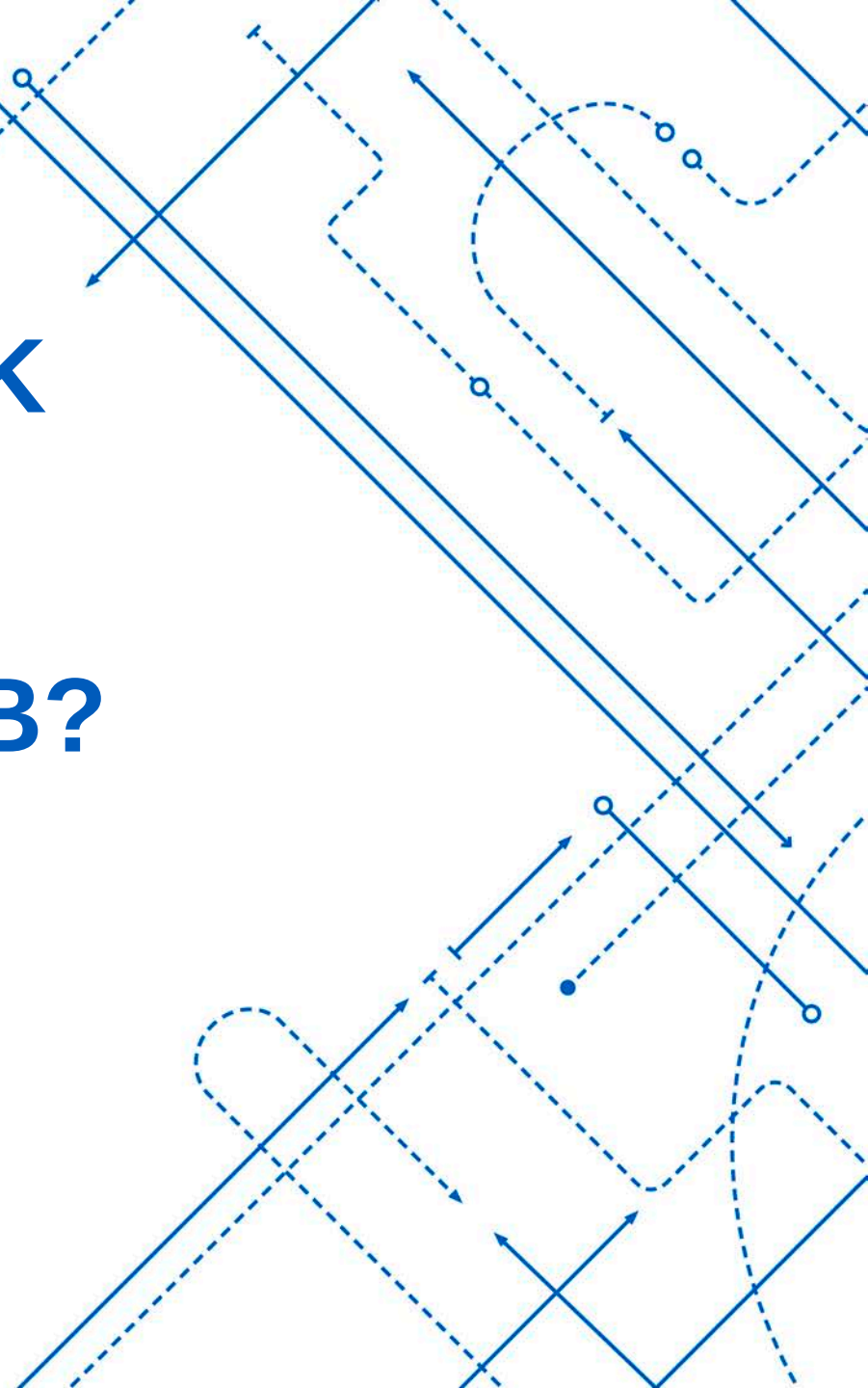
WHAT'S THE RISK OF USING A MOBILE DEVICE FOR WORK AT UB?

Potential Liability and Pitfalls Using a Mobile Device for Work

Dr. Catherine J Ullman
Senior Information Security Analyst

Brian T. Hines
Records Management Officer

University at Buffalo The State University of New York



Our Data is Our Responsibility

UB is responsible for our data no matter where it resides. However, we may not have control over all of the data for which we are responsible. (i.e.; mobile phones, tablets, gmail, personal servers, drop box, etc.)

- Data Classification:

http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/data-classification-standard.html

- Category I: Private regulated data (SSN, passport #, Credit card #, bank account#, etc.)
- Category II: Regulated data subject to FERPA or other federal, state, or business regulation; non-FOILable data (FOIL = Freedom of Information Law)
- Category III: All other non-public data.
- Category IV: Public data

Issues with Using a Mobile Device for Work

- Ownership
- Security
- Privacy
- Compliance
- Liability

Ownership

- Who owns the device, UB or the employee?
- If owned by UB we can control or dictate what it is used for and what is on the device.
- If owned by employee we cannot dictate what is on the phone.
  - However, we can dictate where and how our data is managed.

Security Standards for Mobile Devices

- ALL Mobile devices must meet minimum security standards for protecting data.
  - Cat I data PROHIBITED to be viewed/downloaded on ANY mobile device
  - Cat II can be VIEWED on device ONLY.
    - If using to view Cat II data:
      - Must have most current firmware
      - Passcode required
      - Auto-lock timeout required
      - Disable grace period for lock
      - Erase data upon excessive passcode failures
      - Enable data protection
      - Erase all data before return, repair, or recycle
      - Enable remote wipe functionality
      - Enable data encryption
  - If using a laptop, there are additional requirements

Security

If we don’t control the data we can’t ensure it is safe or secure.

Regulated private data should not be stored on Mobile Devices.

http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/standards-securing-regulated-private-data.html

Category 1, 2, 3 of data etc.

http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/data-classification-standard.html

Access to Systems through non University networks.

http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/remote-access-admin-system.html

Mobile Device Policy

- Outlines why someone should receive UB owned device or allowance for personal device.
- What is expected of them if they have a device.
- Describes safeguarding information on device.
- UB Data on the device.
- Policy provides for appropriate agreement that should be made with employee prior to mobile device being issued.

From Mobile Communication Devices Policy

> Mobile communication devices used to conduct university business, whether owned by the university or the individual, are subject to these preservation requirements and employees using such devices to conduct university business must comply with preservation and production notices.

Mobile Communication Devices Policy

https://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/mobile-communication-device.html

Mobile Communication Devices Web Page

https://www.buffalo.edu/administrative-services/managing-procurement/commonly-purchased-goods/mobile-communication-devices.html

Compliance

Compliance – We must comply with SUNY, State and Federal laws and regulations. (e.g. NYS Breach Notification Act, HIPPA, FERPA, PCI, FOIL, etc.)

- We may be obligated by policy and/or law to produce documents which we hold.
- We need to make sure data is protected and maintained appropriately.
- We lose control of the data if it is stored on a personal device.
- Our Data is Our Responsibility.

Liability - University

- Fines
  - HIPAA – (protected health information) $1.5M per incident
  - NYS (SSN) – $10-$200 per SSN lost
  - PCI – (credit cards) Loss of ability to conduct transactions
- Lawsuits
  - Lose someone's SSN, they may sue for damages
  - Need to produce all records requested in a subpoena, Freedom of Information Law (FOIL), Taylor Law request, etc., we could face fines or legal action.
- Overhead
  - Setup of call centers to answer questions, buying credit protection, etc
- Reputational concerns – faculty, students, parents, staff, granting agencies
- Growing social expectations due to wide-spread media coverage of identity theft

Liability - Personal

Identity Theft

- Thieves aren't just after the data you have access to, they're happy to take yours too!

Financial Loss

- Use the same password everywhere? Bad idea!
- Direct deposit redirection
- Tax return fraud

Privacy

Privacy – What expectation of privacy does an employee have for University owned device or personally owned device?

- 4th Amendment – right to privacy
- PPPL – Personal Privacy and Protection Law
- Case Law
- Electronic Communications Act

University Policy regarding Computing Systems

Employees should have no expectation of privacy when using University computing systems and networks.

Computing and Network use policy II.g:

> The University at Buffalo reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions to determine if a user is violating this policy or state or federal laws.

University Policy and E-Discovery

University Employees should generally:

1. conduct business using University accounts and devices
2. refrain from using University accounts and devices for personal activities.

From SUNY E-Discovery Procedure:

> University officers, employees, and agents should generally conduct official activities using University accounts and devices. Conversely, University officers, employees, and agents should generally refrain from using University accounts and devices for personal activities. The University shall have a right to inspect and monitor all use of its accounts and devices regardless of whether the use is personal or official.

Information Requests and Personally Owned Mobile Devices

- The University will not search your personal device for records related to an information request.
- Employees have a responsibility to produce any records related to an information request that may be on a personally owned mobile device.
- Text messages are not saved to a University server.
  - Text message could be obtained through a subpoena to wireless carrier.
    - Stored Communications Act

Records Management

- Only keep records that have a Legal, Operational or Historic value to the institution.
  - Delete emails, text messages, etc that do not have a “Legal, Operational or Historic value.”

- Follow the records retention schedules.

  SUNY Schedule
  http://system.suny.edu/compliance/topics/records/records-retention/records-retention-schedule

  State Schedule
  http://www.archives.nysed.gov/a/records/mr_pub_genschedule.shtml

  Research Foundation Policy and Schedules
  http://www.rfsuny.org/media/RFSUNY/Policies/records_management_policy_pol.htm

Summary

- Policy says we should “generally” be doing business using University accounts and devices.
- The University will not search your personal device if we receive an information request but you have a responsibility to produce University related data if asked.
- Our Data is Our Responsibility.
- Security of our data on our mobile devices, in public area, etc.
- Privacy v. University’s need to acquire data or do a search.
- Technology is evolving.
  - A reasonable business practice today may be a liability tomorrow.

Questions?

Dr. Catherine J Ullman
Senior Information Security Analyst
Information Security Office
University at Buffalo
cende@buffalo.edu

Brian T. Hines
Records Management Officer
Policy and Operational Excellence
University at Buffalo
420 Crofts Hall
hines@buffalo.edu
716-645-5464