MANAGING THE RISKS OF MOBILE HEALTH DEVICES

PRESENTED BY:

BEECHER CARLSON
MANAGING THE RISKS OF MOBILE HEALTH DEVICES

Introduction

The explosion of mobile devices, along with the many ways in which these devices can be used, is apparent in all aspects of both personal and professional life. Smart phones, tablets, personal monitoring devices, personal digital assistants (PDAs) and other wireless devices are being used with increasing frequency. These devices enhance communication, facilitate business transactions, monitor fitness and diet, provide entertainment and perform a host of other services that never seemed necessary until we began to experience life without them. In healthcare, mobile devices are becoming equally indispensable. Mobile technology can enhance access to health information for providers and patients as well as assist in the provision and distribution of diagnostic and patient monitoring services. Additionally, the many forms of technology referred to as mobile devices can create new ways in which patients can interact with their providers and, in turn, ways that providers can interact with their colleagues, while coordinating care across the continuum. To reduce the risks of mobile device use and mobile data breaches, the risk manager and privacy and compliance professionals must find a way to allow mobile device use in a manner that enhances productivity. At the same time, they must adopt enterprise-wide mobile security policies and procedures to secure the data being shared through the devices.

There are times when it might be difficult to determine when your personal device is just a smart phone or when it becomes a medical device. That determination may become increasingly important from a regulatory perspective and will be discussed briefly at the end of this article. The primary focus of the article, however, will be on how to identify the risks associated with using mobile devices and how to safely deploy and use mobile technology to enhance patient care while also protecting patient privacy.

Why Mobile Health?

The changing healthcare landscape has forced many physicians, executives and other providers to examine their approach to care delivery and to explore new technology solutions as a means to increase patient participation in their care. The goal is to more seamlessly connect care experiences across the continuum and to facilitate communication during the many transitions in care.

In addition to the benefits associated with using mobile phones to enhance current patient and provider relationships, mobile devices offer additional promise. They can enhance the ability to provide care to those who have been traditionally underserved both nationally and globally.
because they live in remote or underserved areas or because they are unable to access transportation to get to a health facility or provider. They can also enable patients to more closely monitor their own or their family members’ health conditions (hypertension, diabetes, etc.). Mobile devices can also facilitate communications between providers or facilities to foster optimal transitions of care for patients who might be transferring between an acute care setting to a subacute, rehabilitation unit or long-term care facility.

The growth in mobile health also is a result of the increased access to broadband wireless connectivity and the number of individuals who now have access to mobile phones. "It is predicted that by 2015 500 million smartphone users worldwide will be using a health care application. Furthermore, by 2018, 50% of the more than 3.4 billion smartphone and tablet users will have downloaded mobile health applications. Currently, more than 40,000 mobile medical applications are available for download in the U.S. and more are being developed that have even greater promise for the future."i

According to a recent report by the Health Information Management Systems Society (HIMSS),ii almost 83% of the physicians who participated in a survey reported that they had downloaded at least one medical app. Another 33% of physicians and 75% of nurses reported that they used medical apps on smartphones daily as part of their work. Thirty-five percent of the responding hospitals reported currently offering medical apps to patients in the form of patient portals, telehealth services and various forms of remote monitoring. Sixty-nine percent of providers most often use mobile technology to view patient information, while 65% report accessing web-based repositories and services to access health care information. Many organizations reported using mobile health for existing telehealth programs while others reported anticipating both expanding their EHR technology and using mobile devices to enhance care across the continuum.

In a recent issue of Agency for Healthcare Research and Quality (AHRQ) Health Innovations (released July 30th 2014),iii there is not only a discussion of how mobile devices are being used, but also some valuable tool kits to walk providers through the policies and practices that might help to alleviate any risk associated with their use. The report titled “Using Mobile Technology to Enhance Care” describes three initiatives that used mobile technology in various ways to improve care management. The programs include one that designed tablet-based software for home visits and care coordination to reduce readmissions, another that coupled care management with text messaging to improve adherence among patients with diabetes and a
Managing the Risks of Mobile Health Devices

third on how mobile devices were used as part of an electronic case management system that improved field nurses’ ability to serve at-risk families.

The featured Quality Tools which are part of this report include a web site, http://toolkit.techandaging.org/toolkit/toolkit-mhealth, for providers with toolkits and resources on using technology to assist care coordination, a mobile-accessible tool designed to help primary care clinicians identify appropriate preventive services, a web site that provides guidance on the adoption of mobile technology in health care and a mobile health program that delivers personalized text messages to help individuals improve and manage their health.

Clearly there are benefits that can be achieved through use of mobile technology. However, there are risks that must be managed as well. Careful planning and specific limits should be considered so that the risks do not outweigh the benefits.

What are the Risks Associated with Mobile Device Use?

There is no argument that there are many benefits that can come from the use of mobile devices and that many efficiencies can be created, but, given the highly private (and protected) nature of what is often transmitted using these devices, there are also many risks. Without the existence of a secured network which stores all of the information being shared breaches in privacy can occur and can be very costly. Data breaches involving mobile devices are increasingly common. In the past year, 80% of organizations have experienced a mobile security incident, 60% of those organizations experienced a loss of $100,000 or more. In most large organizations, the reported losses reached $500,000 or more. According to information gathered by Varonis, a provider of access, governance and retention solutions, mobile devices - especially bring your own devices (BYOD) - have posed significant risks for organizations. “For example, the company found that:

- 50% of employees report that someone at their company has lost a device with important data on it;
- 22% percent said that the lost device had security implications for the organization; and
- 86% of employees are “device obsessed,” using their personal devices to work both day and night.”

“Careful planning and specific limits should be considered so that the risks do not outweigh the benefits.”
Managing the Risks of Mobile Health Devices

In another survey conducted by Forrester Research, Inc., IT security decision makers whose organizations had a data breach in the past 12 months were polled and reported that 36% of the breaches occurred due to “inadvertent misuse by the insider”. Of interest in this category was the fact that, in the public sector and in the healthcare industry, inadvertent misuse by insiders jumped to 44%.vi Thirty-two percent of the breaches occurred due to loss and/or theft of the device, ranking it the second leading cause of breaches.

According to another recent report from Forrester Research, Inc, organizations are allocating, on average, 17% of their security technology budgets towards maintaining data security. vii As the threats that can be inherent in the use of mobile devices in the health care setting become more complex, IT staff, privacy officers, risk managers and clinicians will need to balance the benefits achieved through the use of these devices against the risks created. They will need to spend time and money on developing policies and practices governing use, educating all staff about the risks, creating a secure space for storage of any information containing PHI captured through use of the device and determining if they wish to mandate that only organization owned devices can be used. As always the case, organizations will need to determine whether they incur the cost of issuing organization owned devices and how to manage staff that refuse to be held accountable to the policies and procedures created.

Security Issues Associated with Data Storage

There are no reports nationwide of business data being compromised. When this happens to any personal data, the consequences can be devastating. When it includes compromising personal health information (PHI), the consequences can be even more significant and jeopardize both the organization and the patient. Since mobile devices also can store login credentials and other data that that can be used by hackers and criminal syndicates to gain access to other information they may place the organization at even further risk.

Another serious concern contributing to data breaches is the use of consumer cloud or other file sharing solutions. In our personal lives, we have become accustomed to using file sharing services such as Dropbox, Box or Evernote to store and automatically sync information across devices. These services also enable multiple users to share files. These services are easy to use and familiar to health care providers so they may use them unaware of the risks they pose when PHI is involved.

What Makes Mobile Devices So Vulnerable?

One culprit that is adding to the vulnerability of mobile devices is the increase intrusion of malware. From early 2012 to early 2013, mobile malware grew by an astounding 614%. viii
Trojan horses and other malware installed on mobile devices can log key-clicks and steal login credentials and other data. In its 2013 Data Breach Investigations Report, Verizon found that 40% of data breaches involved malware and 76% involved stolen or compromised access credentials. Verizon also found that 71% of attacks targeted user devices specifically, including mobile devices.  

In health care, many incidents have been reported where medical researchers travel with their computers or portable devices and leave them behind, have them stolen or are otherwise compromised. The Privacy Rights Clearinghouse, http://www.privacyrights.org, is an excellent online resource to read about all cases reporting breaches on privacy in the healthcare industry. Reviewing these claims periodically will enable the risk manager or privacy officer to anticipate the types of risks emerging and will assist them in developing proactive strategies for managing similar occurrences in their organizations.

Issues associated with Portability

What makes these devices so convenient also adds to their vulnerability. Developing habits of immediate response can create expectations for both patients and colleagues. These expectations must be managed proactively so as not to create unrealistic expectations of immediate responses.

In addition, the very fact that these devices are portable means that they can be easily lost, left in a place where the data they contain is not protected and viewed in settings by other than the intended viewer.

Managing the Risks Associated with Mobile Device Use

It will be necessary to strategically plan for how the organization can manage these risks. Devising a comprehensive policy and educating all staff on the risks of using mobile devices will be essential if you wish to avoid the costly breaches experienced by others in the health care industry. Therefore, it is necessary to design a proactive educational program that sensitizes providers to the types of risks that these devices and apps might pose and the specific rules in which the organization has put in place to minimize risks to both patients and providers.

The initial question that you might ask is whether the organization will supply the mobile device to its employees or allow them to use their own device. Although a bring your own device (BYOD) policy is often preferred because it limits the number of devices that a person needs to
Managing the Risks of Mobile Health Devices

carry with them, it can make the device a bit harder to control. Whatever the policy is related to BYOD’s, the education surrounding the use of any mobile device needs to be enforced with the same concerns about privacy and security.

A draft policy is attached that could form the basis for your program. You will need to customize it so that it complies with state laws and reflects the various ways in which mobile devices will be used to support your organization’s business objectives.

**Education**

Planning a comprehensive education module for all staff should also be developed. All staff should be required to complete this education prior to using any mobile device. At a minimum, the program should address the following:

- What is Personal Health Information?
- What are the risks associated with PHI getting in the wrong hands?
- HIPAA Basics: Medical Privacy in the Electronic Age
  https://www.privacyrights.org/HIPAA-basics-medical-privacy-electronic-age
- Review of Recent Cases involving Mobile Devices where Privacy Breaches have Occurred -- http://www.privacyrights.org,
- The Use of Medical Apps and the consequences of downloading them on to mobile devices
- Review of the Organizations Policy
- Consequences for Failing to Comply with the Policy
- References and Resources https://www.privacyrights.org/HIPAA-basics-medical-privacy-electronic-age#17

**Systemic & Strategic Risk Reduction Strategies**

In order to reduce the risk of mobile device data breaches and to optimize the use of these tools while also keeping workers productive, one must adopt a proactive strategy. Similarly, designing systems that enhance the patients’ experience while not exposing them to privacy breaches requires careful thought and planning. As is often the challenge, enterprise risk managers will need to find that careful balance where appropriate tools are accessible when needed, but where a comprehensive organization-wide policy controls all aspects of mobile device use. The following goals should form the basis of this strategy:

- **Security of Data is Paramount** - To assure provider productivity, patient access and data security, organizations should create private cloud-based file sharing services to
manage the sharing of files through a service that is fully under the control of the IT department. To assure that employees are not tempted to use more risky public cloud services (Dropbox or Box for example), IT should block the ports used by these services. Education must be provided to all users so that they fully understand the risk that can be created if they fail to adhere to the organizations policies regarding data storage and file sharing. The enterprise risk manager, chief privacy officer and IT staff should work together to create a private cloud-based sharing system which will facilitate the sharing of all necessary files through a system fully under the control of the IT and privacy staff. Administrators should block the ports used by services like Dropbox to assure that staff do not attempt to use their devices in a manner that is outside the acceptable policies of the organization. Since data may be passing to individuals outside the system, care should be taken to use encryption that is consistent with the standards set by National Institute of Standards and Technology (NIST), www.nist.gov.

- **Create Secure Containers** - “If personal devices are being used by providers, it is advisable to create secure containers for enterprise data. Storing work and patient related data in a secure container shields that data from interference or malware infection that might come from personal data such as games and other consumer apps, photos, music tracks and personal documents received as attachments. Secure containers make it easier for IT administrators to monitor and control shared business related data without intruding on the privacy of employees who are using their personal mobile devices for work.”

- **Require Strict Password Conventions** - The organization’s IT department should be able to establish policies and procedures that specify the strength and duration of passwords which will be needed to access any mobile devices. If passwords are not changed in a manner that is consistent with these policies, devices should be capable of being remotely disabled. This ability to remotely disable devices will also be necessary if mobile devices are lost, stolen or otherwise get into the hands of unauthorized individuals.

- **Create Strict Policies Regarding the Use and Downloading of Medical Applications** - The popularity of mobile health apps is evident: as of March 2013, there were 97,000 mobile health applications available across major application download services and 59% of patients in emerging markets use mobile health applications and services. Health care professionals must be advised of the risks in not only developing their own apps but also of downloading apps onto their own devices which are made by
Managing the Risks of Mobile Health Devices

others or are commercially available. Although the habit of downloading apps may be common in one’s personal life, when used for the delivery of health care, the risks can be significant and include unintended HIPAA violations and the introduction of malware which can compromise the integrity of enterprise-wide data. A process should be in place whereby individuals can request approval of specific new apps. The review and approval of these apps can be part of a multi-disciplinary process involving members of the legal, risk management, privacy and IT team. IT staff should have the authority to remotely disable apps that have been downloaded to personal devices without approval and which are used while conducting business for the enterprise.

**Risk Financing or Risk Transfer**

Risk managers should review their cyber policy to make sure that all of the exposures related to the use of mobile devices are covered. Obviously, even if you are able to transfer some of the financial risks, you will need to be aware of the reputational risks that may be created when patients’ privacy has been breached. The goal should be to manage the risk rather than merely transfer it.

**Incorporate Best Practices from Others When Developing Your Policies**

AHRQ has developed four toolkits that are available online and one is specific to the use of mobile devices to manage chronic disease and to access health information through mobile networks and devices. These toolkits contains valuable information and deployment strategies on eight areas and serve as both an excellent starting point as well as a periodic review of progress made by the organization. The eight areas covered that are in these toolkits include:

1. Program planning
2. Technology Management
3. Patient Management
4. Clinical Management
5. Financial Management
6. Administration
7. Marketing
8. Evaluation & Performance Improvement
Is there a Need to Regulate Mobile Devices?

The Food and Drug Administration (FDA) is the federal agency that has the responsibility for assuring the safety of both pharmaceuticals and medical devices. Although the sophistication of these devices has continued to evolve and many mobile apps now perform functions that are performed by regulated devices, the FDA has been careful to take the position that the only apps which will be regulated are those that could present a substantial risk to patients if they do not work as intended. If the device actually is used to assist in making a diagnosis, it may fall into the category where FDA regulation is warranted. For example, an app which would serve to convert a smart phone into an EKG machine would likely be considered a device subject to FDA regulation. Whereas an app which tracks steps walked and calories consumed per day would not be subject to FDA regulation.

A second regulatory concern might relate to whether the Health Insurance Portability and Accountability Act (HIPAA) would govern the use of mobile devices. The general rule is that if the device is used by an individual it would not be covered by HIPAA. However, if the device allows for the communication between patients and providers and includes the sharing of protected health information (PHI), then HIPAA would apply.

Conclusion

The regulation of mobile devices is complicated and requires input from many disciplines within the organization. No doubt, the use of mobile technology in health care will continue to grow. It will be paramount that organizations develop a strategy that evaluate the effectiveness and manage the risk without creating an undue burden for patients and providers.

---

i Royal Netherlands Academy of Arts and Sciences
Jan 31, 2013 - Mobile phone health applications Guidance for Mobile Medical .... (September 2013).37 A


Managing the Risks of Mobile Health Devices


xii http://toolkit.techandaging.org (accessed 7/24/14)
xiid http://toolkit.techandaging.org/toolkit/toolkit-mhealth (accessed 7/28/14)
xiv http://toolkit.techandaging.org/toolkit/toolkit-mhealth

xv www.fda.gov

ACCEPTABLE USE OF COMPUTING AND TELECOMMUNICATIONS RESOURCES

Policy number: xxx-xxxx
Effective Date: June 13, 2014

1. APPLICABILITY

This policy applies to all users of XYZ Hospital (XYZ) computing, telecommunications and wireless resources, including, but not limited to, computers, computer systems, networks, portable digital assistants (PDAs), telephones, pagers, cellular phones, smart phones, electronic tablets, wireless cards, and two-way radios, whether affiliated with XYZ or not, and to all uses of those resources, whether on hospital premises or from remote locations. These resources are hereinafter referred to as “Computing and Telecommunications Resources.” Additional guidelines or directives may be established by XYZ to apply to specific computers, computer systems, networks, or applications.

2. REQUIREMENTS

A. LEGAL

A user of Computing and Telecommunications Resources shall comply with all federal, state, and other applicable laws; all applicable hospital rules and policies; and all applicable contracts and licenses. Examples of such laws, rules policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit “hacking”, “cracking”, and similar activities; Federal Communication Commission regulations; applicable Internal Revenue Service Regulations; XYZ’s Code of Conduct; the XYZ sexual harassment policy; and all applicable software licenses. Users who engage in communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
B. AUTHORIZED

A user of Computing and Telecommunications Resources shall use only those resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before accessing any computing resource.

Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by XYZ. A user of Computing and Telecommunications and Resources shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access other persons’ accounts does not, by itself, imply authorization to do so.

C. REASONABLE

A user of Computing and Telecommunications Resources shall respect the finite capacity of those resources (including for example; bandwidth, disk space, and CPU time) and limit use so as not to consume an unreasonable amount of those resources, or to interfere unreasonably with the activity of other users.

D. PERSONAL

A user of Computing and Telecommunications Resources shall not use those resources for personal commercial purposes or for personal, financial or other gain, except as may be authorized by the organization.

Incidental personal use of Computing and Telecommunication Resources for other purposes is permitted when the use:

- Does not unreasonably consume those resources;
- Does not interfere with the performance of the user’s job or other job related responsibilities;
- Does not consume an unreasonable amount of the user’s time;
- Does not concern subjects inappropriate in a work or study environment (e.g. accessing pornographic web sites);
• Does not result in unauthorized use or disclosure of confidential information, including protected health information, through use of electronic media such as blogs, podcasts, discussion forums, and other social media;
• Is consistent with the organization’s mission of healthcare, education, research, and community service; and
• Otherwise is in compliance with this and other organizational policies.

E. E-MAIL AND ORGANIZATIONAL COMMUNICATIONS

Announcements, bulletins, and documents deemed by management to be of value and interest to the well-being of employees are an integral part of the system. All broadcast e-mail (unsolicited e-mail sent to more than 50 employee addresses across departments) must be submitted and approved by Strategic Communications, except:

• As otherwise authorized by collective bargaining agreements;
• As otherwise authorized by Strategic Communications;
• As deemed necessary by the leader or executive sponsor or individual organizational units or other organizational partners for the purpose of facilitating business communication; and
• As otherwise provided for in the Emergency Preparedness or Emergency Response program.

In all cases, messages of a strategic nature or in response sensitive matters related to the hospital’s business should be developed in collaboration with the Strategic Communications and Public Relations Department.

All communications over the e-mail system facilitated by any form of technology shall be appropriate for the workplace. Organizational e-mail may not be used for personal solicitations or advertising or other activities. Propagation of chain letters is specifically prohibited.

Falsifying e-mail headers (e.g. providing a false sender’s address) or routing information so as to obscure the origins of mail or mail routes is forbidden. Altering the content of a message attributed to another is not permitted unless the changes are explicitly noted.
F. REPRESENTING THE ORGANIZATION

A user of Computing and Telecommunications Resources shall not state or imply that they speak on behalf of the organization or use organizational trademarks and logos without authorization to do so. Affiliation with the organization does not, by itself, imply authorization to speak on behalf of the organization. Authorization to use organizational trademarks and logos on Computing and Telecommunications Resource may be granted only by the Strategic Communications Department. The use of appropriate disclaimers is encouraged.

3. SECURITY

XYZ employs various measures to protect the security of its Computing and Telecommunications Resources and of their users’ accounts. Users must comply with the XYZ Information Security Policies and Directives and with the organization’s Information Security Guidelines. Users must engage in applicable “safe” practices. For example, establishing appropriate access restrictions for their accounts, keeping the network virus-free, safeguarding passwords, ensuring proper physical safeguards, and protecting the confidentiality of electronic protected health information. In addition to the directives and guidelines referenced in this policy, users of telecommunications resources such as personal digital assistants (PDAs), smart phones, electronic tablets, or similar personal devices who are using a personal device for business purposes must comply with XYZ’s Managed PDA Security Policy and Information Security Directive.

All users must follow the Confidentiality of Health Information policy, and only use encrypted XYZ owned or encrypted XYZ approved personally-owned electronic media to access electronic protected health information, unless an organization approved exception is in place.

4. EXPECTATION OF PRIVACY

A. GENERAL

Computing and Telecommunication’s Resources are not private. For example, communications made by means of these resources are subject to relevant state Law to the same extent as they would be if made on paper. The normal operation and maintenance of computing and telecommunications resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.
B. REASON TO ACCESS ACTIVITY

In addition, XYZ may access or monitor the activity and accounts of individual users of Computing and Telecommunications Resources, including individual log in sessions and communications, with notice, when:

- The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
- It is necessary for XYZ work and business-related reasons (e.g. a person is on vacation or sick leave and access to some files is needed to further institution business);
- It reasonably appears necessary to do so to protect the integrity, confidentiality, availability, or functioning of XYZ generally or computing and telecommunications resources in particular, or to protect XYZ from liability;
- There is reasonable cause to believe that the user has violated, or is violating, XYZ policy;
- There is reasonable cause to believe that the user is engaging in unlawful activity;
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring activity and usage patterns; or
- It is otherwise required by law.

Any such access or individual monitoring, other than that specified in 4.A and B.(1) above, required by law, are necessary to respond to perceived emergency situations, must be authorized in advance by three of the following individuals: Human Resources Director, Legal Counsel, Chief Information Officer, and Information Security Officer. The head of the unit which employees the individual will be notified of such access when appropriate. XYZ, at its discretion but subject to any applicable laws, may disclose the results of any access or monitoring, including the contents and records of individual communications, to appropriate XYZ personnel or law enforcement agencies and may use those results in XYZ disciplinary proceedings and/or legal proceedings.

C. MONITORING AS A JOB OR SERVICE REQUIREMENT

XYZ may also authorize access and monitoring of an employee’s or agent’s actual communications over its computing and telecommunications resources where customer service is a primary responsibility of an employee’s job duties. Such monitoring must be
authorized by the Human Resources Director and employees in positions subject to monitoring shall be notified of such activity.

5. REMOTE ACCESS TO XYZ COMPUTING RESOURCES

- XYZ employees and students may be authorized for secure remote access to information assets owned by or in custody of XYZ. Remote access may be granted by the department director or other appropriate authorizing authority where appropriate to fulfill a person’s work or other responsibilities.
- Remote access for contractors, business partners, referring physicians, other health care providers or other approved users with significant business justification may be approved on a case-by-case basis by an appropriate authorizing authority.
- Applicants for remote access must submit the XYZ Remote Access form. Information technology support vendors may also be granted remote access for system and application maintenance as negotiated in the support contracts.
- Noncompliance with the requirements of a remote access authorization or with other provisions of this policy, as determined by the authorizing authority, may result in immediate loss of access privileges and possible corrective or legal action against the violator with notification.

6. ENFORCEMENT

Users who violate this policy may be denied access to computing and telecommunications resources and may be subject to other penalties and disciplinary action, both within and outside of XYZ, including any actions authorized by security policies or any policy applicable to personal devices. Violations will normally be handled through XYZ procedures applicable to the relevant user. However, XYZ may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so to protect the integrity, confidentiality, or availability of XYZ or other computing resources or to protect XYZ from liability.