UNIVERSITY OF PENNSYLVANIA HEALTH SYSTEM Health Services Policy and Procedure Manual	**Number:** **ISD-SEC-03**
Subject: Acceptable Use of Information Resources Policy	**Page 1 of 5** **Effective:** **11/4/19** **Reviewed:** **12/31/2022** **Restricted**

Purpose

The purpose of this policy is to inform workforce members of Penn Medicine (University of Pennsylvania Health System and Perelman School of Medicine), and other authorized third parties who access Penn Medicine electronic resources, of their responsibilities related to the acceptable use of Penn Medicine owned and/or managed electronic information resources, technology, and systems.

Scope

This policy applies to all Penn Medicine entities, departments, and workforce members, as well as any authorized third parties who access, store, use, transfer, transport, produce or dispose of electronic information resources, technology, and systems owned and/or managed by Penn Medicine. This policy also applies to any electronic devices connecting to all Penn Medicine networks or systems, other than Penn Medicine sponsored guest networks. This includes, but is not limited to, computers, systems, technology equipment, software, networks, copier/fax equipment and the handling of email, voice mail, Internet, television, telephone, or other electronic information.

Workforce members includes employees, physicians, house staff, volunteers, trainees, and other persons whose work performance is under the direct control of Penn Medicine.

This policy is applicable to all components and entities of UPHS including but not limited to: the Hospital of the University of Pennsylvania ((HUP); an unincorporated operating division of The Trustees of the University of Pennsylvania (Trustees)); Presbyterian Medical Center of the University of Pennsylvania Health System d.b.a. Penn Presbyterian Medical Center (PPMC); The Pennsylvania Hospital of the University of Pennsylvania Health System (PAH); Chester County Hospital; Chester County Health and Hospital System; Wissahickon Hospice d.b.a. Penn Medicine at Home; Clinical Practices of the University of Pennsylvania (CPUP); Clinical Care Associates; Princeton HealthCare System (Penn Medicine Princeton Health and Penn Medicine Princeton Medical Center); Lancaster General Health (LG Health) and Lancaster General Hospital (LG); the Hospital of the University of Pennsylvania Reproductive Surgical Facility; the Surgery Center of Pennsylvania Hospital; the Endoscopy Center of Pennsylvania Hospital; the Surgery Center at Penn Medicine University City, a facility of Penn Presbyterian Medical Center; the Penn Medicine Radnor Endoscopy Facility, all ambulatory care facilities (ACF) that are off campus departments of PPMC operating in New Jersey, and all divisions, facilities and entities within UPHS that have a CMS Certification Number (CCN) or that are operating under the license of a UPHS entity (collectively the "Entities"); and the Perelman School of Medicine (PSOM), except where specifically noted.

Policy

Penn Medicine electronic information resources, technology, and systems shall be used for authorized purposes only consistent with the research, education, and clinical care mission or business related activities of Penn Medicine. By using or accessing Penn Medicine's electronic information resources, technology,

and systems, the individual agrees to comply with this Policy as well as all applicable federal, state, and local law and regulation.

Individuals shall not use sensitive or restricted information for personal gain nor in any manner that would be contrary or detrimental to the welfare of Penn Medicine. Sensitive or restricted information is defined by the Data Classification Policy.

> Sensitive (High Risk) – a) Protection of the data is required by law/regulation and Penn Medicine is required to report to the government and/or provide notice to the individual if the data is inappropriately accessed; or b) The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on Penn Medicine's mission, safety, finances, or reputation or the loss would have a significant adverse impact on any individual.
>
> Restricted (Moderate Risk) – a) The data is not generally available to the public; or b) The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the Penn Medicine's mission, safety, finances, or reputation or the loss would have a mildly adverse impact on any individual.

Individuals shall not infringe upon the intellectual property rights of others including plagiarism and unauthorized use or reproduction.

E-mail, Internet access, and other Penn Medicine information resources are tools that Penn Medicine has made available for Penn Medicine business purposes. However, limited personal use of these resources, as defined by management, may be permitted in special circumstances. Management is responsible for determining at what point non-business use becomes a violation of policy or affects an individual's job performance.

All information and communications residing on Penn Medicine information systems is the property of Penn Medicine, and any individual granted access to these information assets should be aware that users have no expectation of privacy when using Penn Medicine information resources, technology, and systems. All use of electronic communications is subject to monitoring, logging and auditing. As part of an investigation of any violation of law, regulation, operational issue, or Penn Medicine policy, procedure, or standard Penn Medicine reserves the right to examine or copy any information residing on Penn Medicine systems without prior consent or notification to the individual.

All members of the Penn Medicine workforce are responsible for information security at Penn Medicine and must participate in the Penn Medicine Security Awareness Program by completing required training and adhering to the practices conveyed in regular security communications.

Information Access

Access to Penn Medicine information and information systems must be limited to the level of access that is needed by an individual to perform his or her job functions and must be approved by management. Violations include but are not limited to:

- Accessing or using information assets, including sensitive or restricted patient or business information, without authorization.
- Sharing your password or using another individual's password.
- Automating the login process in an unauthorized manner.
- Misusing software to hide personal identity, or interfere with other systems or users.
- Using privileged access for purposes not related to official duties.

Computing Resources

Penn Medicine workforce members, and other authorized third parties that access Penn Medicine electronic resources, are responsible for using information systems in a professional, ethical, and lawful manner and also protecting information resources from unauthorized access. Computing resources shall only be used for their intended purposes. Each individual is responsible for the actions taken with his or her User ID and password while logged into a system. Violations include but are not limited to:

- Leaving computer system accounts open and accessible when you are not physically located at the workstation.
- Leaving a portable computing device unattended in a public area.
- Storing unencrypted sensitive or restricted information on a computing device including desktop computer, laptop, USB or other external storage, or other device.
- Using any Penn Medicine computing device, located in a clinical patient care area, to access any web site or any information that is not directly related to clinical care or other Penn Medicine business related activity.
- Using Penn Medicine information systems to operate a personal business, for personal gain in any form, for personal use (other than limited incidental use), or for other inappropriate use.
- Downloading non-business related information including, but not limited to, unauthorized applications, music, videos, or games.
- Degrading system performance, depriving access to a Penn Medicine resource, or gaining access to a system or information for which proper authorization has not been given.
- Unauthorized access to electronic information or resources.
- Modifying systems or application settings without authorization.

- Accessing, viewing, displaying, sending, storing, printing, or otherwise disseminating material that is sexually explicit, suggestive, pornographic, profane, obscene, threatening, discriminatory, harassing, fraudulent, offensive, defamatory, or unlawful.

Remote Access

Remote access to computing resources within the Penn Medicine network shall use an approved method as outlined in the Remote Access Standard, based on the type of connectivity required. Violations include, but are not limited to, using unauthorized remote access methods or technologies such as unauthorized wireless access points, pcAnywhere, VPNs, GoToMyPC, etc.

Software Downloads and Security Protections

All third party software to be installed on Penn Medicine networks will be reviewed by Information Services Platform Engineering and/or Information Security. Using or copying software in violation of a license agreement or copyright laws is prohibited.

Penn Medicine computing devices shall utilize endpoint protection software. Prohibited actions include but are not limited to:

- Disabling, or attempting to disable, endpoint protection, anti-virus protection or any other security solution.
- Creating or propagating computer viruses, worms, ransomware, or other malicious code.

E-Mail and the Internet

When using e-mail or Internet-based communications, individuals are acting as representatives of Penn Medicine. Personal e-mail accounts, such as Gmail, Yahoo, etc. must not be used to conduct business on behalf of Penn Medicine. As is the case with all Penn Medicine information systems, e-mail and Internet communications are not private, and workforce members have no expectation of privacy related to usage. Violations include but are not limited to:

- Making a network connection to a personal service, for example personal cloud storage, while connected to the Penn Medicine network.
- Intentionally intercepting, recording, reading, or deleting another individual's e-mail without proper authorization.
- Sending sensitive or restricted information outside the Penn Medicine network without securing the information using an Information Security approved solution.
- Intentionally attempting to send or sending unsolicited junk mail, "for profit" messages, or chain letters.
- Automatically forwarding e-mail to an external account.
- Creating an unauthorized VPN-type connection with a remote service.

Device and Media Control
Sensitive information must be securely removed from electronic devices and/or media when it is no longer needed or under Penn Medicine control. If this is not possible, the storage media must be destroyed. Corporate Information Services controls the disposition of computing devices and media and will provide assistance. Violations include but are not limited to:

- Duplicating sensitive or restricted information without appropriate authorization.
- Disposing of computing devices and/or media without removing data from the media using an approved Penn Medicine data sanitization solution.

Confidentiality of Data
Individuals must never transmit sensitive or restricted information in clear text over a public network (for example public Wi-Fi) and must use encryption when sending Penn Medicine sensitive or restricted information to an external recipient. Violations include but are not limited to:

- Accessing or using information stored or processed by Penn Medicine for unauthorized purposes or permitting anyone else to make unauthorized use of such information.
- Disclosing or disseminating the contents of any sensitive or restricted information to any person except as authorized or permitted in the conduct of their work assignment.
- Violating local, state, federal and international laws as applicable.

Enforcement
The Penn Medicine Information Security Office (IS Security) is authorized to limit and/or terminate network access for individuals and/or devices that do not comply with this policy.

Revision History

Version	Date	Author (Changed by)	Changes
1.0	11/4/2019	Andrea Thomas-Lloyd	Superseded 7/11/2011 policy
2.1	12/31/2022	Michael Moran	Reviewed without substantive changes

Supersedes: 7/1/2011 and ALL RELATED EXISTING POLICIES	**Issued By:** **Kevin B. Mahoney** **Chief Executive Officer**