ADVOCATE HEALTH		
Title: Enterprise Acceptable Use Policy		**Document Number: 58170**
Document Type: ☒ **Policy** ☒ **Procedure** ☐ **Guideline** ☐ **Other**		**Last Review/Revision Date: 03/18/2025**
Content Applies to Patient Care: (Select all that apply) ☐ **Adults** ☐ **Pediatrics (Under 18)**	**Content Applies to: (Select One)** ☐ **Clinical** ☒ **Administrative**	**Effective Date: 03/18/2025**
Scope: ☒ **Enterprise** ☐ **MW Region** ☐ **SE Region** ☐ **WI** ☐ **IL** ☐ **Greater Charlotte Market** ☐ **Navicent Market** ☐ **Wake Market** ☐ **Floyd Market** ☐ **Entity Only (Entity Name):** ☐ **Department Only (Department Name):**		

I. PURPOSE

The purpose of this policy is to outline the acceptable use of data within the Digital Landscape. Inappropriate use exposes Advocate Health to an increased risk of cybersecurity, regulatory, legal, and reputational harm.

II. SCOPE

This policy applies to Advocate Health Inc. entities and to all data and Technology Assets owned or controlled by Advocate Health. This policy applies to all users such as teammates, faculty, vendors/contractors, consultants, students, temporary, volunteers, and other users at Advocate Health and its subsidiaries.

III. DEFINITIONS/ABBREVIATIONS

Advocate Health Network: All physical and logical connections providing connectivity between or within Advocate Health owned, leased, or managed facilities. The Advocate Health Network includes, but is not limited to, all logical intranets and extranets as well as physical analog lines, leased lines, frame relay circuits, fiber optic cabling, premise wiring, wireless, cloud infrastructure, or other associated network wiring and equipment.

Collaboration Technology: Software, platforms, or services that enable users at different locations to communicate and work with each other. These tools may include capabilities for document management, recording, whiteboarding, chat, real-time contributions, and other collaboration-oriented activities.

Data: Any data as defined by the *Enterprise Data Classification Policy*.

Digital Landscape: All hardware, software, data, and processes associated with the Advocate Health Network, Technology Assets, or hosted applications in a cloud environment.

Mobile Device: Any easily transportable device that can be used to store information or connect to the Advocate Health Network and/or Internet, including but not limited to laptops, tablets, smart watches/exercise trackers, and smart phones.

Payment Card Information (PCI): Any data as defined by the *Enterprise Data Classification Policy*.

Personally Identifiable Information (PII): Any data as defined by the *Enterprise Data Classification Policy*.

Protected Health Information (PHI): Any data as defined by the *Enterprise Data Classification Policy*.

Removable Media: Any easily transportable device that can be used to store data, including but not limited to optical discs, portable media players, removable static memory, external hard drives, and USB drives (i.e.: thumb drives).

Technology Asset: A physical and logical device owned, leased or used pursuant to contractual rights by Advocate Health that can store, process or transmit data. This includes, but are not limited to, PCs, tablets, Mobile Devices, terminals, laptops, servers, mainframes, printers, faxes, copiers, telephone systems, private branch exchanges, lab instruments, uninterruptible power supplies, network devices, wireless devices, biomedical devices, storage media, and back-up devices.

Users: Advocate Health teammates, affiliates and their Workforce Members, contractors, third party vendors, and other approved users of Advocate Health Technology Resources.

Workforce Members: Employees, volunteers, trainees, and other persons whose conduct in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

IV. POLICY

A. User Responsibilities

1. Each user will use Advocate Health Technology Assets responsibly, professionally, ethically, and lawfully. A user's ability to access these resources does not imply a right of access. Users must only access Advocate Health Technology Assets for which they have authorization.
2. Each user will be responsible for the security of the Information Environment. This responsibility extends to the content of the communications the user generates, disseminates, or solicits through any Advocate Health resource. This can include, but is not limited to, written reports, email, messaging, postings, file transfers, voicemail, images, verbal, and other communication.

3. Each user will be responsible for ensuring their use of external computers and networks (e.g. the Internet, personally owned devices, home networks) does not adversely impact the cybersecurity of the Advocate Health Information Environment or data.
4. Each user will be responsible for ensuring all work completed for Advocate Health remains organizational property unless otherwise approved by the appropriate leader. This property must remain with Advocate Health upon a user's departure. For instance, the creation of a document or a computer program while employed by Advocate Health is considered Advocate Health property and must remain with Advocate Health.
5. Each user who uses, manages, or views Payment Card Information (e.g. credit cards, debit cards, etc.) will be responsible for ensuring they are following the requirements outlined in the *Enterprise Payment Card Industry Data Security Standard Policy*.
6. Each user will be responsible for the security and protection of their access credentials. Users will be responsible for all activity completed under their access credentials.
7. Each user will be responsible for handling data, including Protected Health Information (PHI), via Technology Assets in accordance with all Privacy and Data Governance policies, which are to be read together with this policy. For instance, users must not copy, transfer, misrepresent, or alter any PHI in an unauthorized manner.
8. Each user will be responsible for adhering to this policy and will be periodically informed of its requirements. For more information about your role in securing our environment, please contact Cybersecurity and Privacy for resources designed to protect our patients.

B. Authorization for Use

1. Users must use and disclose data in a manner consistent with organizational policy and approved procedures.
2. Users will only be authorized to use approved Technology Assets and accounts when conducting business, including clinical duties, on behalf of the organization.
3. Users will only be granted access to information systems after they have been properly vetted through Human Resources or other authorized onboarding processes.
4. Users will only be given access to information systems that are required to perform their job duties and to which they need to know. Management will be responsible for determining, requesting, and authorizing the information system(s) their teammates need to access in order to complete their job functions. Users should not have system privileges that exceed their role.
5. User access to information systems may be modified due to administrative actions (e.g. transfer, change in job description, etc.).
6. User's access to all information system resources will be terminated promptly in the event of a user's separation from the

organization. Obligations of confidentiality continue after termination.

7. Users who require remote access to information systems must follow authorized procedures and technologies.
8. Users must use only authorized remote access solutions to connect to and access the Advocate Health Network.
9. Users working remotely must not hide their working location, including any network source addresses (e.g. a private VPN). Only those locations authorized by the user's manager and Human Resources are permitted, and any violation can include penalty up to termination.
10. Users will be required to accept an information system login or acceptable use agreement (where utilized) before being granted access to an information system.
11. Cybersecurity reserves the right to deny or revoke access privileges of any device or user at any time, if there is reasonable belief that a cybersecurity or privacy incident has or may occur.
12. Cybersecurity reserves the right to monitor, inspect, or search any information system, including data, at any time.
    a) Technology Assets are provided for business purposes only. Users should have no expectation of privacy associated with the use of these information systems.
    b) This monitoring may take place with or without the consent, presence, or knowledge of users.
    c) Monitoring may be conducted in consultation with or the authority of Privacy, Legal, Human Resources, or Risk Management as appropriate.
    d) Cybersecurity may modify information systems to remediate active attacks.
    e) Cybersecurity retains the right to remove any material it views, in its sole discretion, as offensive, inappropriate, or potentially illegal.

C. Acceptable Use

1. Users will be responsible for exercising good judgment regarding appropriate use of data, electronic devices, and network and computing resources in accordance with applicable policies and standards.
2. Users will be issued access credentials that consist of a unique user identifier(s) and password and must comply with policies covering account management and supplemental standards. Whenever technically feasible, these credentials will be required for the use of technology.
3. The external release of data involving non-public data, including into cloud-based resources, must utilize approved procedures. This may include, but is not limited to, vendor onboarding requirements, the creation of appropriate agreements, which may include a Business Associate Agreement, and the use of authorized Technology Assets.

4. The use of authorized encryption technologies will be required when transmitting non-public data outside of the Advocate Health environment. Encryption should be utilized internally, where possible, to protect the storage and transmission of data.
    a) Users communicating with patients via Mobile Device-based software may only utilize Advocate Health approved software with all required security measures.
    b) Any encryption used must be in alignment with policies covering encryption and any supplemental standards.
5. Transmitting full Social Security Numbers should be avoided whenever possible, particularly if being sent externally. Any email containing Social Security Numbers must be encrypted using an Advocate Health approved encryption method, even when being sent within the Advocate Health internal network where technically feasible. All processes utilizing a Social Security Number must adhere policies covering minimum necessary and disclosure requirements.
6. Any external (e.g. non-Advocate Health) individual acting in the role as another covered entity that obtains PHI will be solely responsible for the protection of the data, including ensuring its proper disposal. In the event the data becomes compromised through that person's or their Workforce Member's access, use, maintenance, or disclosure (including through use of security codes or access through Advocate Health resources), responsibility for such events will be that of the non-Advocate Health person and not Advocate Health.
7. Users must take all reasonable and prudent measures and will be responsible to ensure the safety and confidentiality of all PHI downloaded to any communications device. Users may be directed to have additional measures by Privacy and/or Cybersecurity.
8. The handling and use of digital media (e.g. audio, photography, video, recordings, etc.) must comply with enterprise policies. For instance, applicable consents must be obtained prior to using digital media involving users, patients, and/or their families by following policies and procedures defined by Privacy.
9. Users must only communicate with patients using an authorized Advocate Health solution, though communications should be routed through the patient portal (e.g. MyChart) whenever possible. Unencrypted communications may only be sent to patients when all required authorizations, consents, and/or acknowledgements are obtained, except as stated below.
    a) Unencrypted emails may be sent to patients only if they have requested the email be unencrypted and have confirmed they understand the risks of unencrypted communications.
    b) Certain appointment reminder emails may be sent unencrypted if they are limited in data, sent to the patient's email address on record, and equivalent to what would be left as an appointment reminder on the patient's voicemail.

c) Please reference Privacy policies on safeguarding Protected Health Information for more information.

10. Users must identify themselves honestly and accurately when communicating with others. For example, users must not alter the "From:" line or other attributes of origin data in email, messages, or other postings.
11. User emails will be retained for 2 years, and peer-to-peer instant messaging conversations will be retained for 30 days.
12. Users will be responsible for taking appropriate precautions when accessing email and websites. For instance, users must use the latest phishing guidance before clicking on suspicious links or attachments within communications.
13. Users should only use Advocate Health-approved technologies as the means of connection to the Advocate Health Network.
14. Technology Assets are intended to be used for authorized purposes only and all data stored on these systems will be the property of Advocate Health.
15. Users will be responsible for properly securing all data, including the physical security of Technology Assets, electronic devices, and other media. This includes, but is not limited to, the following:
    a) Users will be required to lock or log off information systems when unattended.
    b) Users must take all reasonable and prudent measures to physically secure all Technology Assets.
    c) All clinical devices used to transmit, store, or process non-public data must be secured in an appropriate location. This includes, but is not limited to, being in a secured area/location, locked storage bin, locked computer closet, or other lock down means.
    d) Mobile Devices and other portable devices (e.g. cameras, recording devices, Removable Media) must be in your possession and not be left unattended in an insecure location.
    e) Any device used to store non-public data (ex: laptops, servers, Removable Media, cameras, recording devices, etc.) should be inventoried and labeled properly to include the owner of the data and/or contact information.
    f) When transported, Mobile Devices and Removable Media should be stored in a locked vehicle's trunk, where available, and should not be left in the trunk overnight or for long durations. Never leave items lying in a vehicle that are visible from the outside. Users will be responsible for all media, equipment, and data they remove from Advocate Health property, even for work purposes.
    g) Users must immediately report any lost or stolen Advocate Health Technology Asset, as well as personally owned devices using authorized means to connect to non-public

data. This includes any camera, recording device, or other media containing patient images or non-public data.

h) All keys used to store equipment and/or non-public data should be properly secured (e.g. not left in plain sight, unattended, or in an open drawer).

i) Please reference the applicable physical security department(s) further guidance on physical security controls.

16. The use of office equipment (e.g. copiers, printers, scanners, fax machines, etc.) must utilize a secure configuration where appropriate. This includes, but is not limited to, the following:
    a) Office equipment that contains flash memory and/or a hard drive must have appropriate safeguards in place to minimize exposure of non-public data when the equipment is moved, disposed of, lost, or stolen.
    b) Any security features inherent to the equipment such as drive encryption, concealing job names, and data overwrite/wipe must be enabled.
    c) Rented or leased equipment must be sanitized before being returned to the vendor in accordance with policies covering the disposal and reuse of electronic media.
17. Users must only utilize approved Collaboration Technology.
    a) Users will be expected to use caution when sharing a desktop through Collaboration Technology.
    b) Any recordings with PHI or other non-public data must be properly stored and secured in accordance with the *Information Security Policy* and other policies covering photography, video, or audio recordings.
18. Mobile Devices (corporate and personal) must adhere to applicable Information Technology and other organizational policy prior to accessing information systems. Mobile Devices may be used outside the premises of the organization and must follow authorized procedures.
19. The occasional, limited, appropriate personal use of Advocate Health Technology Assets will be permitted based on management approval and when the use does not: (1) interfere with the user's or any other user's work performance, (2) violate any corporate value or Advocate Health policy, and (3) increase the risk of a cybersecurity incident.
20. Non-public data should only be stored on Advocate Health or authorized assets. Any exceptions to this must utilize approved encryption technology.
21. Any storage media (e.g. memory cards, film, Removable Media, etc.) with non-public data must be disposed of in accordance with policies covering the disposal and reuse of electronic media.
22. Any information system, including personal devices authorized for use, may be compelled during an investigation, litigation, or other legal matter to be produced or imaged. Users must comply with any request for devices.

23. The use of artificial intelligence (e.g. machine learning, large language models, etc.) must comply with all enterprise policies regarding compliance, privacy, cybersecurity, and data use, and adhere to any guidance for use established through data governance and related committees. Any applicable oversight, review, and approval must be completed prior to implementation and use, and re-evaluated periodically based on risk.
24. The creation and use of QR codes must comply with the branding and approval conditions established by Information Technology.
25. Users have a duty to report any suspicious activity as well as any activity that they may have performed that could potentially compromise the security of the organization's systems.
26. Users will be required to act according to the *Information Security Policy* and all its subordinate policies and standards.
27. Users may consult Information Technology to ensure all policies, procedures, guidelines, and standards are followed.

D. Prohibited Activities

1. The use of Technology Assets for inappropriate or unlawful content and purposes is prohibited. All conduct will be expected to align with the defined organizational values and workplace policies.
2. No user may access Advocate Health resources by logging in as another user or using a session already logged in by another user.
3. The sharing of user access credentials is prohibited. Also, the use of another user's access credentials is prohibited. Credentials include but are not limited to passwords, multi-factor authentication (MFA) tokens, smart cards, hardware encryption keys, tap-and-go badges, ID badges, and any other solution that is designed to authenticate a user.
4. Users must not attempt to circumvent authentication procedures on any information system or otherwise attempt to gain unauthorized access.
5. Users must not:
    a) Reveal their user password to anyone.
    b) Reveal a password on questionnaires.
    c) Write passwords down and store them in plain view (e.g. anywhere in office or on paper).
    d) Store passwords outside of an authorized password manager/vault.
    e) Use the same password for business and personal purposes (e.g. work password for online shopping/banking).
    f) Violate requirements outlined in policies on account management.
6. Users will be prohibited from using corporate identifiers for the creation or use of personal accounts (e.g. using an Advocate Health email for a personal social media account, ordering personal products, signing up for a personal newsletter, etc.). Corporate identifiers may be used for the creation or use of business-related accounts.

7. Users must not use Advocate Health Technology Assets or data for personal or commercial profit, operate a business, solicit money for personal gain, distribute chain letters, conduct political campaigns, or any otherwise engage in non-Advocate Health use.
8. Users will be prohibited from using Technology Assets to store or transmit personal data (e.g. pictures, music, videos, financials, etc.).
9. The use of unsanctioned cloud-based applications, personal cloud document storage, or backup services is prohibited.
10. The use of personal domain names to conduct Advocate Health business is prohibited. All purchased domain names must go through authorized purchasing procedures, which may include consultation with business units such as marketing.
11. Users must not monopolize, disrupt, or waste Advocate Health Technology Assets. Prohibited activities include, but are not limited to, sending non-business emails, subscribing to non-business mailing lists, unapproved streaming, personal social media use, and playing games.
12. The use of Advocate Health assigned equipment by family members and friends is prohibited.
13. Users will be prohibited from automatically forwarding email outside the entity. It is inappropriate for members to indiscriminately route incoming email from a corporate account to an account outside of Advocate Health.
14. Unauthorized tampering of a corporate email banner or footer is prohibited. Users must review the warning banner prior to clicking links contained within an email.
15. Users will be prohibited from using personal email accounts and web-based e-mail (e.g. Google Gmail, Yahoo Mail, Hotmail, Spectrum, school addresses, etc.). Personal email accounts must not be utilized to conduct Advocate Health business. This includes sending non-public data to a personal email account managed by the teammate. Advocate Health will not be responsible for the security practices of non-Advocate Health covered entities, health care providers, and other third parties.
16. The sharing of non-public data with those that do not have a need to know is prohibited.
17. Users will be prohibited from releasing data to an external party without the proper authorization as referenced by *Enterprise External Data Authorization Request (EDAR) Policy*.
18. Texting patient PHI is not permitted except as specifically permitted by this policy and using authorized messaging solutions. Any clinically-relevant data must be documented in the approved system of record.
19. The recording of webinars or other forms of online presentations that contain non-public data is prohibited unless all persons accessing the recording have a valid need to know and it is retained only for the minimum necessary period.

20. Users will be prohibited from making unauthorized payments on behalf of the organization. Advocate Health will not be responsible for any unauthorized charges (e.g. costs, identity theft, or other fees) incurred by a teammate.
21. Users will be prohibited from electronically signing any document unless authorized by the *Enterprise Financial and Signature Approval Policy*.
22. All personnel specifically accessing cardholder data (PCI) will be prohibited from copying, moving, or storing cardholder data onto local hard drives and/or electronic media. The use of email to transmit cardholder data is also prohibited.
23. Smart devices should not be used as a camera where non-public data may exist, unless the photos and recordings are taken within a secured, authorized application (e.g. Rover, Haiku, corporate phone).
24. Users will be prohibited from purchasing, installing, or servicing Technology Assets without prior authorization.
25. Users must not open or attempt to open the encasement of any Technology Asset unless part of authorized responsibilities. Users are not to circumvent any locking mechanism that secures a device or its components.
26. Users must not add unauthorized components to Advocate Health Network or Technology Assets.
27. Users will be prohibited from utilizing any camera functionality on a Mobile Device (corporate or personal) while operating a motor vehicle.
28. Users must not alter Technology Asset configurations, settings, or functions unless authorized. Examples include but are not limited to the adjustment of login screens, passwords, anti-virus software, encryption software, distribution software, time-out settings, screensavers, or other settings.
29. Users must not maliciously destroy, delete, or otherwise damage any hardware, data, or software licensed, owned, leased, or possessed by Advocate Health. In addition, Advocate Health reserves the right to seek compensation through legal action for any damage maliciously caused by the user.
30. Only authorized applications and/or licensed software will be installed on Technology Assets.
31. Users will be prohibited from unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from publications, copyrighted materials (e.g. music, books, etc.) or other copyrighted sources.
32. Users must not violate copyrights, terms of use, or license agreement of any software or service. The installation and use of licensed software must go through the appropriate Information Technology approval process.
33. Users may not do any of the following without prior approval from Information Technology:

a) Copy software for use on home computers.
b) Provide copies of software to any non-Advocate Health entity.
c) Download and install unauthorized software on any computing device (e.g. crypto wallets, browser extensions, private VPN, personal applications, and file storage)
d) Download software, games, ringtones, apps, etc. that result in a cost to Advocate Health. Reasonable personal use of non-business-related software on Advocate Health-owned smart phones will be permitted as long as it doesn't interfere with the operation of the device, adversely impact the Advocate Health Network, or violate any other provision of this or any other Advocate Health policy. Software downloads should be limited to commonly available commercial products from reputable app stores to minimize the potential for infections from malware or viruses from unknown sources.
e) Modify, revise, transform, or adapt any licensed software.

34. Users will not use information system audit tools unless specifically authorized by Cybersecurity. This includes, but is not limited to, network mapping, network discovery, port scans, traffic analysis, traffic logging, discovery techniques, or any other data gathering processes.
35. The use or distribution of hacking or malicious software is strictly prohibited unless authorized by Cybersecurity. Examples include but are not limited to system hacking, password cracking (guessing), file decryption, bootleg software copying, or similar attempts to compromise or circumvent security measures. Any violation will be considered a cybersecurity incident.
36. Users must not support illegal activities as defined by federal, state, or local law. This includes, but is not limited to, hacking, social engineering, gambling, intercepting data on the network, use of "pirated" software, export controls (e.g. encryption), and other fraudulent activities.
37. Users must not engage in illegal or any conduct that interferes with the rights of others or the ability to provide service(s). This includes, but is not limited to, cyberstalking, libel, harassment, invasions of privacy, consumer fraud, unauthorized dissemination of trade secrets or intellectual property, violation of trademark laws, or transmittal of commercially restricted data.
38. Users will be prohibited from using Technology Assets without proper cybersecurity controls installed.
39. Users will be prohibited from paying ransomware fees to recover any data. Cybersecurity incidents will be governed by policies concerning incident response and recovery, including the *Enterprise Cybersecurity Incident Response Team Policy,* which will evaluate ransom demands.

40. Users will be prohibited from transmitting non-public data via their personal device except through authorized applications. This includes, but is not limited to, artificial intelligence, data scraping, screen capture, optical character recognition, transcription, or other online services.

E. Violation or abuse of this policy may be grounds for corrective action, up to and including employment or contract termination as well as possible civil and criminal penalties. Violations will be referred to Human Resources, Office of Student Affairs, Faculty Services, Privacy, Legal, or Law Enforcement, as appropriate.

F. Corrective action and teammate counseling will be administered according to policies on sanctions and applicable teammate counseling/corrective action policies by Human Resources.

G. Policy exceptions may be requested for all Cybersecurity policies and standards where a business need arises. Requests must have a documented requester, risk assessment, policy in conflict, reason/justification, compensating controls (if possible), and approval from the requester's management. Exception approvals are granted by the CISO or appointed designee for a maximum period of one year.

V. CROSS REFERENCES

- Enterprise Cybersecurity Incident Response Team Policy
- Enterprise Data Classification Policy
- Enterprise External Data Authorization Request (EDAR) Policy
- Enterprise Financial and Signature Approval Policy
- Enterprise Payment Card Industry Data Security (PCI DSS) Standard Policy

See other relevant policies related to:

- Compliance
- Human Resources
- Information Technology
  - Cybersecurity
  - Data Governance
- Privacy
- Treasury/Finance
- Legal

VI. RESOURCES AND REFERENCES

HIPAA	164.310(b): Workstation Use 164.310(c): Workstation Security – R 164.308(a)(5): Security Awareness and Training

NIST-800-53 R5	AC-2, AU-13, CA-7, CM-10, CM-11
PCI_DSS_v3.2.1	12.3.5; 12.3.6; 12.3.7
NIST CSF v. 2.0	DE.CM-03
Illinois Compiled Statutes	(625 ILCS 5/12-610.2) Sec. 12-610.2. Electronic communication devices. https://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=062500050K12-610.2

VII. ATTACHMENTS

Not Applicable