AD571

Subject	AD571 - EpicCare Link Policy for Third Parties		
Category / Section	Administration / Corporate Compliance		
Owner	Zack Kaiser (Corp Compliance Administrator)		
Reviewer(s)	Dir - Regional Outreach Services		
Approver(s)	APM Administrators, LJ Fallon (Exec VP & Chief Legal Officer)		
Effective Date	11/22/2022	**Review Frequency**	• 1 Year
Approval Date	12/02/2022		

Scope of Policy/Procedure ***(applies to entities/locations marked below)***

X This document applies to **all** entities/locations listed below

	Hospitals		Ambulatory/Off-Campus locations		Other Carle Entities
	All Carle Hospitals listed below:		All Carle ambulatory/off-campus locations listed below:		All other Carle entities listed below:
	Carle Foundation Hospital (Urbana CFH)		CFH/CPG ambulatory locations *(also includes Home Health, Therapy Services, Medical Supply, Danville Surgicenter, Specialty Pharmacy)*		Arrow Ambulance, LLC
	Carle Hoopeston Regional Health Center (CHRHC)		CHRHC ambulatory locations *(includes, CARMC, Cissna Park, Danv-Fairchild, Mattoon-Hurst, Milford, Rossville, Tuscola, Watseka)*		Carle Retirement Centers *(Windsor of Savoy & Windsor Court)*
	Carle Richland Memorial Hospital (CRMH)		Champaign SurgiCenter, LLC		Health Alliance Medical Plans
	Carle Eureka Hospital (CEH)		Administration Building locations (includes Carle at the Fields)		FCC – FirstCarolinaCare Insurance Co.
	Carle BroMenn Medical Center (CBMC)		Carle West Physician Group (CWPG)		CHPP—Carle Health Physician Partners
			CRMH Ambulatory locations (includes Bridgeport, West Salem, Olney, Specialty Services)		Carle Cancer Institute Normal, LLC

☐ **Scope Exclusions** *(Mark this box and enter any departments or locations within a marked entity that are exempt from the policy/procedure.)*

ATTACHMENTS

PURPOSE

A. To establish expectations regarding an EpicCare Link (MyPatient portal) users access, use, and/or disclosure of Carle Health patient data to remain compliant with the HIPAA Privacy rule and Carle Health's corporate standards.

DEFINITIONS

A. Personal Information ("PI") – means the following:

1. An individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted, or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:
   a. Social Security Number.
   b. Driver's license number or State Identification card number.
   c. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
   d. Medical information.
   e. Health insurance information.
   f. Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Printed copies are uncontrolled documents. Refer to the intranet for the most current version.

2. Username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

B. Electronic Protected Health Information ("ePHI") – means any protected health information ("PHI"), as defined under HIPAA, which is transmitted by, or maintained in, electronic media.

C. Encryption – A method of encoding data so that only authorized individuals can decode and read the information, using a strong, industry accepted, encryption algorithm.

D. Protected Health Information ("PHI") – means individually identifiable health information that is transmitted or maintained in any form or medium.

E. Workforce – All providers, employees, students, volunteers, agents, and contractors with whom the EpicCare Link entity has direct control.

F. Breach – Improper acquisition, access, use, or disclosure of "unsecured PHI" in a manner not permitted by the HIPAA Privacy Rule. Any impermissible acquisition, access, use or disclosure of unsecured PHI is presumed to be a breach unless Carle can demonstrate that there is a low probability that the PHI has been compromised based on a 4-factor risk assessment.

G. EpicCare Link – an Epic web-based, read only application, for connecting Carle Health to community practices, such as referring physicians. Through EpicCare Link, community users will be given secure access to patient information in the Carle Health Epic data repository. This platform allows Carle to extend patient information to external facilities and improve the continuity of care in our community.

H. Site Administrator – An individual(s) designated to serve as an entity's EpicCare Link administrator who is responsible for changing passwords, editing user demographics, retaining user *Confidentiality and User Acknowledgement* forms, deactivating user accounts, maintaining patient lists (where applicable), submitting new user requests to Carle Regional Outreach, assisting with compliance investigations initiated by Carle or a Community Connect Partner, and validating user employment statuses.

I. User – any individual that has been granted access to Carle's electronic medical record portal, EpicCare Link.

STATEMENT OF POLICY

A. Third Party Access to Electronic Health Records

a. All requests from third parties or vendors affiliated with Carle Health or a Community Connect partner must receive approval from Carle Health prior to establishing a direct or indirect network connection to Carle Health's information systems, including EpicCare Link.

b. A third party may express their interest in EpicCare Link by emailing RegionalOutreach@Carle.com and complete an application.

c. Carle will approve or deny any sites or individual user's access to Carle information systems.

d. At the time the EpicCare Link Confidentiality and Use Agreement is signed, Carle and the site will agree on an appropriate number of users based on business need. Additional users beyond the initial allocation must be approved by Carle.

e. Carle will arrange training for users addressing appropriate use of the portal and provide training materials.

B. User Account Management

a. Each individual that accesses EpicCare Link will be use a unique username and single use password.

b. Portal users are prohibited from sharing their credentials with others. Users and the user's site are responsible for any activity in the portal associated with their users.

c. The Site Administrator is the primary contact for resetting passwords. If they are unable to assist, the user may call Carle's IT Help Desk at (217) 383-4357 or contact their Carle Representative.

d. Accounts that are inactive for a period of one-hundred and eighty (180) days will be disabled.

e. A user's network access may be temporarily revoked as part of an investigation reviewing account misuse, either from account compromise (i.e., stolen password), or malicious intent.

C. Password Requirements

a. As mentioned, a username and password are for the sole use of the individual. EpicCare Link users are prohibited from sharing their password and username with other individuals or use another individual's user ID. Group logins are prohibited.

b. Users are prohibited from saving their username and password to any web browser. Any authorized user must take precautions to safeguard their password.

c. During the initial login, the user will be required to update their password.

Printed copies are uncontrolled documents. Refer to the intranet for the most current version.

d. Passwords, at minimum, must be eight (8) characters long, and include at least one (1) alphabetic character, numeric character, and punctuation character.
e. A user must reset their password every six (6) months.

D. Privacy and Security Awareness Training

a. The EpicCare Link user must conduct security awareness and privacy training programs as required per the HIPAA Security rule. If the EpicCare Link facility's training does not meet Carle Health's standards, Carle may issue training to the EpicCare Link facility for distribution to its users.

E. Adequate Safeguards for Protected Health Information

a. EpicCare Link users must use adequate physical, technical, and administrative safeguards to protect the confidentiality of patient information. Failure to adhere to the standards may result in the agreement being terminated.

F. Remote Access

a. To provide a more secure framework for the EpicCare Link remote access, each user must use Two-Factor Authentication (2FA). The user must choose a method to receive a six digit code that they must enter when they log in. The code can be sent via text message, email, or by accessing the mobile app.
b. Each user will receive a reset code that they will need if they ever need to change authentication methods (such as getting a new phone, new e-mail, etc.). If a user needs to reset their authentication method, they may email MyPatient.Sec@carle.com.
c. Third parties with access must agree to abide by Carle's security standards for securing the network session. This includes terminating the session when completed, as well as guarding against unauthorized viewing and access by means of a password locking screen saver.

G. Minimum Necessary

a. The EpicCare Link entity and its workforce is required by law to limit the amount of protected health information they access, use, request, or disclose to others, to the minimum necessary to accomplish the intended purpose for every transaction except for those disclosures when the minimum necessary rule does not apply.
b. The EpicCare Link entity and its workforce, third party or vendor affiliated with the EpicCare Link facility are not permitted to access protected health information of anyone who is not under their medical care or who is not the subject of a transaction that the individual is processing.
    i. A user may not access a medical record out of curiosity or concern, including their own medical record, family members, coworkers, friends, or anyone else for which they are not performing a job function.
    ii. Users are expected to use normal routes provided to patients if they wish to view their own medical record.
c. When a user encounters a "Patient Select Confirmation" screen, they must enter a reason and comment for accessing the record. They are expected to leave a detailed justification of their business need to access the record.
    i. Choose the "reason" for accessing the record: access needed by patient's PCP, emergency care, referring provider, secondary review, or other.
    ii. Then type a valid "comment" to expand on the need to access. Random letters or numbers are prohibited and may be flagged for audit.
d. In the event Carle becomes aware that a third party may have acted in a manner that does not comply with this Policy, the *Confidentiality Agreement and User Acknowledgment* and/or applicable state and federal laws, whether as a result of an audit by Carle or otherwise, information regarding such action shall be provided to Carle's Corporate Compliance Office. The Corporate Compliance Office shall investigate the circumstances and determine whether any remedial action is warranted.

H. Proactive Monitoring and Privacy Incidents

a. Carle Health's Corporate Compliance department routinely monitors accesses of patient records via EpicCare Link. Epic tracks every click a user makes into a patient's record.
b. Should Carle Health identify an unexplained access or suspicious activity, Carle's Corporate Compliance Office will contact the Site Administrator. They are expected to include the user's leadership and privacy representative to review the concern within ten (10) business days of receiving the request and determine if the user had a business need to be in the record.
c. In the event the Site Administrator and the user's leadership are unable to ascertain a business need, the facility is expected to conduct their own investigation involving the user and notify the Carle Corporate Compliance Office of their findings.
    i. If the user accesses a record without a business need, leadership is expected to notify the Carle Corporate Compliance Office upon discovery.

Printed copies are uncontrolled documents. Refer to the intranet for the most current version.

ii. Carle Health may contact the affected patient(s) to determine if they authorized any user to view their information.
iii. The EpicCare Link site is expected to follow their own policies and procedures and determine if any discipline or education is required for their employee.
iv. The Site Administrator is to notify the Carle Corporate Compliance Office of any corrective action (discipline, education, termination) details that are completed within five (5) business days.
v. The Site Administrator is expected to cooperate in an appropriate resolution and respond to request for information within a timely manner.
vi. It is understood by Carle Health and the EpicCare Link facility that Carle Health will hold the EpicCare Link facility responsible for any wrongdoing of their workforce.

d. Should the EpicCare Link facility identify suspicious activity of a user, they must notify Carle Health's Corporate Compliance department by calling Carle's AlertLine (888) 309-1566. If reporting anonymously, please remember to pick up the "P.I.N" number given and leave as many details as possible.

I. Breach Notification

a. Unauthorized access of data is a reportable event. The access to Carle data in EpicCare Link by users who are not authorized to access that data, or who access information beyond that necessary to fulfil their job requirements, is considered an unauthorized access.
b. If it is determined that the access compromised the patient's PHI, the Carle Corporate Compliance Office will then send written notification to any patient affected sufficiently describing the incident so that the patient can take measures to prevent or mitigate any harm that may ensue.
c. Should Carle Health discover any inappropriate access, we will notify your facility. If necessary, we will also make any reports to: the Office for Civil Rights, the Illinois Attorney General, and the user's licensing body.
d. Breaches or other inappropriate activity may result in termination of the user's credentials without notice or the entire site's loss of access to the portal.

J. Patient Demographic Information

a. If an EpicCare Link user determines that a patient's address or other demographic information is incorrect, the EpicCare Link user must direct the patient to Carle's Financial Services department for assistance.

K. Patient Anonymity Rights

a. Patients may request anonymity for personal privacy and security purposes when admitted to a Carle Health facility. Patients who are a security risk and/or are perceived to be at risk may be protected.
b. EpicCare Link users shall respect the patient's anonymity rights and avoid releasing patient information to news media, family, and friends pertaining to the patient's presence before, during or after the hospitalization.
c. EpicCare Link users shall not acknowledge these individuals as patients of a Carle facility while admitted.

L. Disclosures of Financial, Proprietary or Confidential Business Information

a. EpicCare Link users may never access, use, or disclose confidential business information of Carle Health. Should the EpicCare Link user discover a disclosure of such information, it must immediately contact Carle Health's Corporate Compliance department for proper resolution.

M. Workforce Data Loss Prevention Policy

a. All users are expected to know, understand and apply the requirements of this policy when using EpicCare Link.
b. The Carle Corporate Compliance Office will notify Executive Leadership of sites who knowingly violate this policy or fail to comply with the investigation of any identified violations.

N. Termination of Access

a. Carle Health retains the right to terminate any access to the EpicCare Link system for any reason.

OTHER RELATED LINKS

AD525 - Third Party Access to Electronic Health Record

REFERENCES

Illinois Personal Information Protection Act 815 ILCS 530/1
The HIPAA Privacy Rule- Title 45 Subtitle A Subchapter C Part 164
§164.103- Definitions
§164.308- Administrative Safeguards
§164.310- Physical Safeguards
§164.312- Technical Safeguards
§164.502(b)- Minimum Necessary
§164.506- Uses and Disclosures (treatment, payment, or healthcare operations)
§164.508- Uses and Disclosures (authorization required)

Printed copies are uncontrolled documents. Refer to the intranet for the most current version.

§164.510- Uses and Disclosures (agreement or objection required)
§164.512- Uses and Disclosures (agreement or objection not required)

ELECTRONIC APPROVAL ON FILE

Printed copies are uncontrolled documents. Refer to the intranet for the most current version.