Cerner Patient Portal Privacy Policy

Effective Date: July 20, 2011

Revised Date: June 26, 2019

Overview

Cerner Corporation (Cerner) is committed to protecting your privacy and the security of the information you entrust with us. This privacy policy (Policy) discloses Cerner's information gathering and dissemination practices. Your use of *Cerner Patient Portal* is governed by the terms of this Policy, and by using or accessing *Cerner Patient Portal* you agree to be bound by this Policy.

How the Health Information in *Cerner Patient Portal* is Obtained

Cerner Patient Portal provides a view into your healthcare provider's (Provider's) Electronic Medical Record (EMR) and allows you to communicate securely with your Provider. *Cerner Patient Portal* does not separately maintain or manage your personal health information that is visible to you from within the EMR. The information available for you to view through *Cerner Patient Portal* is not a comprehensive view of all the data in your Provider's EMR.

Information You Contribute to *Cerner Patient Portal*

When you enter information in *Cerner Patient Portal*, that information is stored in your Provider's EMR where it is accessible to members of your Provider's care team and staff based on your Provider's policies and procedures. Information that becomes a part of your Provider's EMR remains in your Provider's EMR even if you should stop using *Cerner Patient Portal*.

Sharing Your Personal Health Information

It is your choice to share your information that is accessible through *Cerner Patient Portal*.

When you share information from *Cerner Patient Portal* with another individual, you acknowledge and accept responsibility for the decision to provide them access to potentially sensitive information.

How We Use Your Information

- Personal Information - Cerner maintains limited information about you, such as your name, date of birth, and medical record number, during your use of *Cerner Patient Portal*; such information is maintained to ensure you are connected to

your medical record. *Cerner Patient Portal* uses your *Cerner Health* identity (user name and password) to confirm your identity when you sign into *Cerner Patient Portal*.

- Site Usage Information - Site usage information may be used by Cerner or its partners to support analysis in support of healthcare research, *Cerner Patient Portal* management initiatives, and understanding of the *Cerner Patient Portal* user base to enable Cerner to enhance *Cerner Patient Portal*. Site usage information is de-identified, meaning your personally identifiable information is removed and cannot be connected to you in any way.
- IP Addresses (Server Log Information) - An IP address is a number automatically assigned to your computer whenever you access the Internet. All computer identification on the Internet is based on IP addresses that allow computers and servers to recognize and communicate with each other. *Cerner Patient Portal* collects IP addresses in order to administer the system, understand and manage site access, and analyze use and demand. *Cerner Patient Portal* also uses IP addresses to identify individuals violating the *Cerner Patient Portal* Terms of Use or who are threatening the service, site, content, users, or others.

Use of Cookies and Single-Pixel GIF Files

Cerner Patient Portal places a text file called a 'cookie' in the browser files of your computer. Cookies are pieces of information that a website transfers to an individual's hard disk for record-keeping purposes. *Cerner Patient Portal* uses cookies during your online session to deliver content specific to your interests. Cookies allow *Cerner Patient Portal* to more efficiently deliver the information you want. The cookies do not contain personal information. If you disable cookies in your browser, you will be unable to log into *Cerner Patient Portal*. In addition to cookies, some web analytics tools used by *Cerner Patient Portal* place a single-pixel GIF file on a computer as a tracking indicator.

Deleting Your *Cerner Patient Portal* Connection

Should you decide that you no longer wish to use *Cerner Patient Portal*, you may delete your connection to *Cerner Patient Portal* from within your *Cerner Health* account. This removes your access to *Cerner Patient Portal* by removing *Cerner Patient Portal*'s ability to use your *Cerner Health* identity (user name and password) for sign-in. Deleting the connection does not notify your Provider that you no longer wish to receive communications in *Cerner Patient Portal*. You must contact your Provider to notify him or her that you no longer wish to receive communications via *Cerner Patient Portal*.

Children's Privacy Protection

Cerner Patient Portal is not designed for or targeted at children. Cerner will not knowingly collect and maintain personally identifiable information from children under 13 years of age.

Compliance

Cerner regularly reviews its compliance with this Policy and as a business associate of your provider, follows your provider's Notice of Privacy Practices. Nothing in this Policy changes anything in your provider's Notice of Privacy Practices. If you have any concerns about how Cerner treats personal information, please contact us at:

Cerner Corporation
2800 Rockcreek Parkway
Kansas City, Missouri 64117 U.S.A.
Attention: Chief Legal Officer

Modifications

Cerner may change this Policy at any time without advance notice to you. However, Cerner will take reasonable steps to notify you of material changes it makes to the Policy. You are responsible for regularly reviewing this Policy. Your continued use of *Cerner Patient Portal* constitutes your acceptance of the revised terms.