# Privacy and Confidentiality Statement

**Kidney Community Emergency Response Coalition (KCER) operated by Health Services Advisory Group (HSAG) knows how important privacy is to its online users and is committed to protecting their information and the security of KCER's websites.**

This Privacy and Confidentiality Statement describes how KCER collects and uses the information received through its web systems. Please review this policy and contact KCER if you have any questions.

**Email:**
KCER@nw7.esrd.net

**Address:**
Kidney Community Emergency Response Coalition c/o HSAG | 3000 Bayport Drive, Suite 300, Tampa FL, 3607

## Information Collection and Use

KCER collects certain information to help run and maintain its websites. For example, information collected provides general statistics about how people use the websites to help KCER continually identify areas for improvement.

KCER will not obtain personally identifying information when users visit the websites, unless they choose to provide such information, such as meeting or portal access or when completing KCER's online participation agreements or project-specific commitment forms. While users do not have to provide personal information to visit KCER's websites, KCER's websites do automatically collect and record certain information about each visitor's computer hardware and software, including:

- The date and time of the visit.
- The web pages visited.
- The type of computer and browser used.
- The search engine used, as well as the keywords that helped the visitor find the website.
- The country where the visitor's computer is located.

KCER is the sole owner of all information collected on its websites. KCER does not sell, trade, or rent user information to other organizations, groups, or entities. Though, information collected on KCER's websites may be shared with government agencies, when contractually required.

## IP Address Log Files

KCER collects and uses IP addresses to analyze trends, administer the site, track user's movements, and gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information, except when the user has chosen to provide personally identifying information when registering for meetings or portal access, or when completing KCER's online participation agreements or project-specific commitment forms. They can, however, be resolved to identify the name of the organization that owns the IP address.

## Meeting Registration and Use

KCER offers online registration for some professional meetings. Users are required to provide contact information during registration. This information may include name, credentials, organization, and email. KCER uses this information to register users for meetings, contact users about meeting news and updates, and to

potentially contact the user about future, related KCER meetings and activities. Required information fields for registration on the meeting website are clearly marked; all other fields are optional.

## Participation Agreements and Project-Specific Commitment Forms

KCER offers online participation agreements or project-specific commitment forms that partners may complete on KCER's website. Users are required to provide contact information during completion of these agreements and forms. This information may include name, credentials, organization, and email. KCER uses this information to sign users up for participation in quality improvement initiatives and specific projects, and potentially contact the user about future, related KCER initiatives and projects. Required information fields for participation agreements and project-specific commitments on the website are clearly marked; all other fields are optional.

## Portal Registration and Use

Registration is also required for access to secure, project-specific online portals maintained by KCER. This information is used to verify the identity of the requesting user and may be used to issue user names and passwords. All portals are secured by passwords and cannot be accessed by unauthorized personnel. Please keep your password confidential. Do not share it with outside entities. In order to ensure your privacy, immediately notify KCER if an employee with access to a portal leaves your agency.

When registering for, or logging in to, a secure portal, information is encrypted and protected with industry standard SSL technology. While on a secure page, the lock icon on the bottom of web browsers, such as Microsoft Internet Explorer, becomes locked.

## The Use of Cookies

A cookie is a small text file websites place on a hard drive to help remind a website who you are and to add convenience to your visit. For example, returning users registering for an event will have their information preloaded on registration forms based on previous visits to the web page. Users can accept or decline cookies. Users who reject cookies can still be able to use the websites; however, some areas of the website may be limited. For example, users may not receive custom information from the website or have their information preloaded into registration forms.

## Email

Every attempt is made to protect personal information that is shared with KCER. However, non-encrypted electronic mail is at risk of being accessed and viewed by other users without your knowledge and permission. Do not use email for any confidential information. KCER is not responsible for the security of email communications. To protect privacy, users may send confidential information through postal mail to KCER.

## Information Sharing

KCER may share information about the use and engagement of its websites with some of its customers, such as the Centers for Medicare & Medicaid Services (CMS) and some state governments. KCER does not provide personally identifiable information in these reports, which are generally used for verifying the level and type of use of KCER websites.

## Links

KCER websites contain many links to other sites. KCER is not responsible for the privacy practices of other sites. Users should be aware when they leave the KCER website and should read the privacy statement of each website

that collects personally identifiable information. This privacy statement applies solely to information collected by KCER websites.

## Information Security

SSL encryption is used to protect sensitive information online. KCER servers are kept in a secure, restricted-access environment. Robust encryption technology/protocols are in place to ensure the security of user information. Ongoing training on security and privacy practices is provided to KCER staff members.

## Notification of Changes

KCER reserves the right to amend this policy, as necessary, without prior notice. Any changes to the privacy policy will be posted on the website so users are always aware of what information is collected, how it is used, and under what circumstances, if any, it is disclosed. If, at any point, a decision is made to use personally identifiable information in a manner different from that stated at the time it was collected, KCER will notify users by way of email. Users will have the choice as to whether or not to give KCER permission to user their information in this different manner. Unless specific information is given, KCER will use information in accordance with the privacy policy under which information was collected.