Accessing King County HMIS in the Field: A Practical Guide for Agencies

1. Set up Two-Factor Authentication (2FA) on Mobile Device

In January 2018, King County HMIS switched from PKI certificates to 2FA. This change increases security in order to better protect client data in HMIS. Additionally, it makes it easier for users to access HMIS from mobile devices (since there's no more PKI certificate to install). Detailed directions for setting up 2FA on a device can be found by following this link.

You have two authentication options:

- **Use an authenticator app.** This is an app you download onto your cell phone, such as Google Authenticator or Microsoft Authenticator. Once you download the app, you'll be prompted to scan a QR code on the screen.
- **Get a code emailed.** A code will be emailed to the email address associated with your account in HMIS. This is the easier option.

2. Secure Mobile Device

Lost or stolen devices are the biggest concern when it comes to using mobile devices to handle sensitive data. Because Clarity Human Services is entirely web based and does not store client data locally on the device (i.e. there is no offline access), this is less of a concern for HMIS. That said, a limited amount of residual data may be stored on the device in the form of cached pages and form autofill data stored by the browser. To help mitigate this, we suggest the following:

- **Encrypt all devices**. This functionality is built into the latest versions of both Android and iOS.
- **Access from a "Private" Browsing Window.** Accessing Clarity Human Services from a private browsing window (eg . an "incognito" window in Chrome) or changing the browser's settings to not store form data (aka "autofill") or page caching (not possible on all pages).
- **Enable Device/Profile Management**. Both iOS and Android include functionality that allow you to locate and, if necessary, wipe lost or compromised devices.

3. Pay Attention to Surroundings

Unlike in the privacy of an office, using devices in the field may inadvertently expose client data to others able to view the screen. A few considerations:

- **Set policies for when it is and is not appropriate to share screens.** Although there are times where it might be helpful to share a screen while working with a client in HMIS (eSignatures, assessments, etc.), other areas of the system may expose the private data of other clients. Agency policies should be very clear when this is allowed and when it isn't. Please assure that installing and using HMIS on a mobile device aligns with your agencies cell phone use policies, data protection policies, and your HMIS Agency Lead has been informed.
- **Consider Privacy Screens**. If appropriate you can buy privacy screens for most major phones/tablets that prevent viewing from side angles.

4. Secure the Connection

Connecting to the Internet via unsecured or third-party wireless hotspots may expose client data. Ideally, you should:

- **Use a secure connection you control**. Use a built-in cellular connection or a cellular wifi hotspot with an encrypted connection.
- **Use a VPN.** Using a VPN connection will help improve the security of the connection.

Need more help? Contact the King County HMIS Help Desk: 206-444-4001 x2; kcsupport@bitfocus.com