El Paso HMIS
Steering Committee Meeting
“The More You Know”

April 2023

epchomeless.org

What Will Be Covered?

- Clarity Feature Update – April 2023
- Security & Attacks
- How to keep information secure
- What to look out for while using HMIS
- Conclusion/Questions

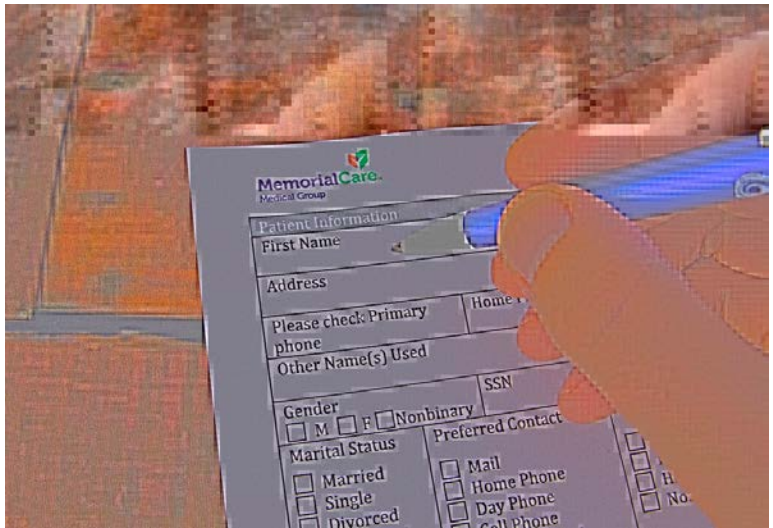
Clarity Update-No Update

- No new update for April 2023.
- Updates to our Looker system have been completed.

No Update This Month! Look for next update in May 2023.

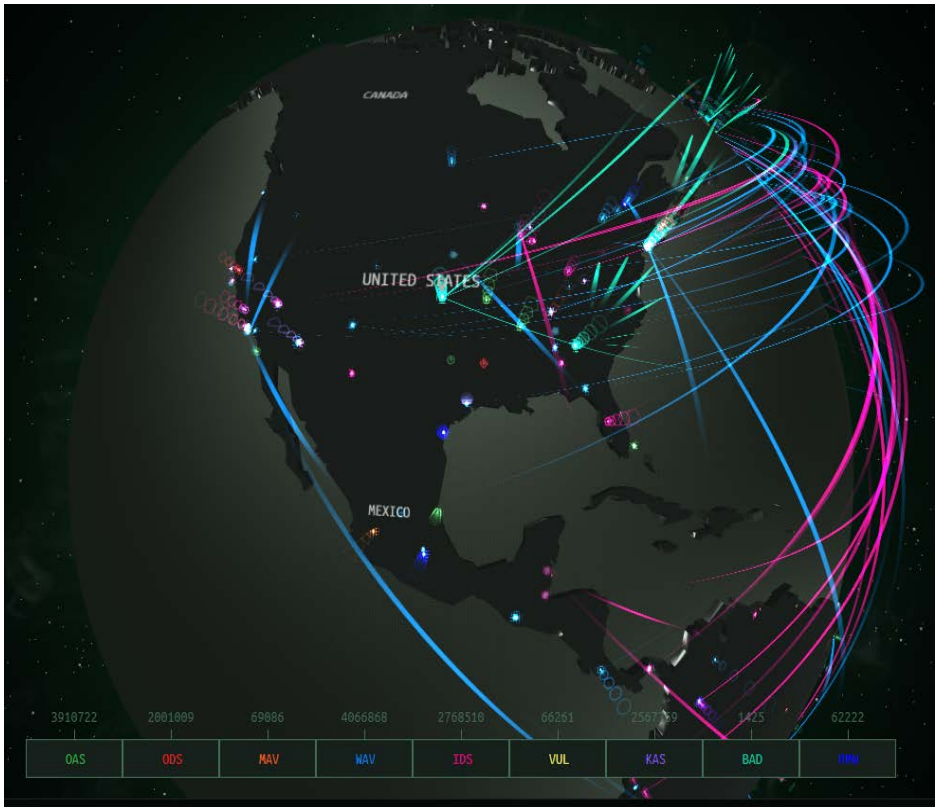
Security of systems with HMIS

- HMIS contains very sensitive information including Name, SSN & DOB
- This can also include address, telephone number, email address, income and other aspects.
- All HMIS users and agencies must keep PPI secure at all times.
- Loss of data must be reported to the HMIS lead and HUD immediately!



Attacks on systems

- Attacks to database systems happen every day.
- Attacks on various systems including Health Management Systems in Hospitals, Airline Systems, Social Security Administration, or anywhere information is stored.
- Successful attacks happen because of one or two things….
  - Either a system is not protected due to configuration issues, bad software or major vulnerabilities.
  - Is due to a user of the system who does not take necessary steps to keep the information secure or is an internal threat.(Insider threat)



HMIS Security

- It takes us all to keep the information in HMIS secure.
- Bitfocus takes all the necessary steps to make sure the system is as secure as possible.
- This includes updating the system when needed and monitoring the systems 24/7
- Since Bitfocus has 20,000+ users, we as users must take the necessary steps to keep the system and all information secure as best as possible!

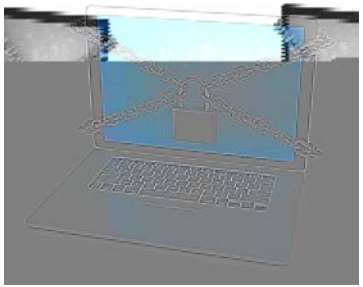
Our Community

20,000+
Active Users

4,000+
Agencies

How to keep information secure?

1. **Never share your username and password to anyone! EPCH or Bitfocus will never ask you for your password. Bitfocus will only ask you for your username to verify your access.**
2. **Never leave your computer unattended while using HMIS. Having any information on your screens while your away allows anyone to see or steal the information.**
3. **Always lock your computer when leaving your desk. This helps to make sure no information is showing on your screen for others to see. (for Windows: WIN+L) (Apple: CTRL+Command+Q)**
4. **If you print out any information, either store it in a file & filing cabinet OR destroy the information by using a shredder or a document bin.**
5. **Never share any information to people outside of your organization. Even a little information is enough if it gets in the wrong hands.**



Additional Security Steps

1. **Keep your computer up to date. Updates by Windows or Apple always include security updates for your system.**
2. **Never save your Username & password on your web browser (Chrome, Edge, Firefox, etc.) Saving your password gives easy access to anyone who gets onto your system.**
3. **Internet browsers must also be kept up to date. Check periodically for updates in the settings of your browser.**
4. **Always look for a "Lock" icon when visiting sites & using HMIS. That icon means that website is secure to use. Any site that is NOT secure can harm your system, infrastructure or HMIS.**
5. **Always make your password as long and as difficult as possible. The more special characters in the password, the more secure it is.**
6. **Make sure you have an antivirus program on your system. Weather it's a paid version or free version, it's always good to have running in the background and keep your computer protected.**

What to look out for?

- **Run a virus scan on your computer from time to time. Viruses are normally hidden and are hard to find. The scan will "quarantine" any threat and will keep your computer safe.**
- **Phishing emails can harm your computer and any system. Always look at the email addresses of email's coming in. If it looks odd or you're not sure if its real, always contact the organization and person via phone to verify.**
- **Spear Phishing is when emails are directed at a specific person. Whaling is when an email targets high profile employees like CEO's, Directors & senior personnel.**
- **Vishing is when someone calls an organization acting as company or important individual to get information from you. Always ask for credentials and verify by calling that company back asking about their employment status and reason.**
- **Social Engineering is when someone talks to an employee to gain specific information. This can be dangerous especially if someone is looking for a client with DV history. Never give out information unless it is necessary for the sake of the client.**

Conclusion

- It is everyone's responsibility to keep information safe
- Always make sure your computer and antivirus is up to date. This helps to keep HMIS, your computer and your infrastructure safe.
- Look out for those key details when odd emails, phone calls or persons come into your organization. Always verify.

Any Questions?

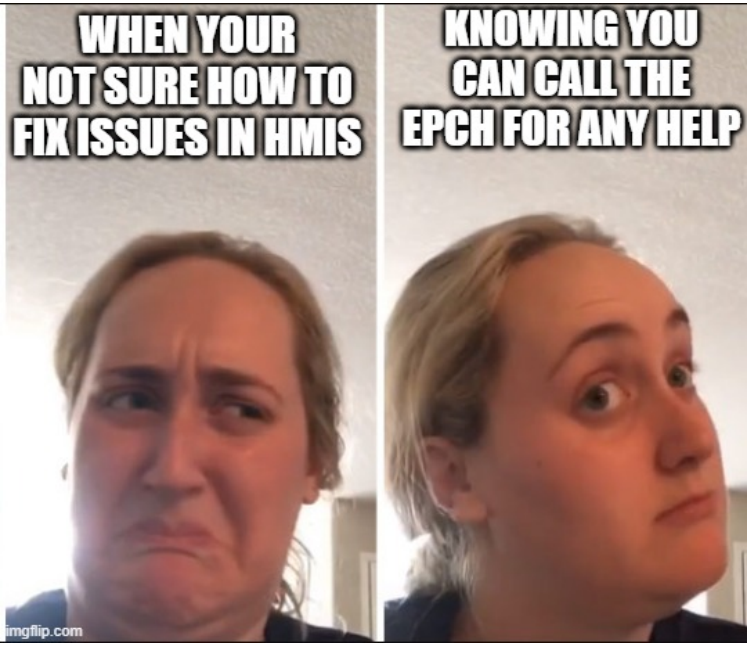
EPCH HMIS “Eyes on the Fries!”

HMIS Zoom Lunch Meeting!

- **Open to anyone who needs help or has questions with HMIS!**
- **Zoom meeting will be from 11:30am-1:30pm**
- **Next meeting is on Friday 4/28/23!**
- **Bring your questions, concerns and lunch!**
- **Hosted by Denver Herald (HMIS Tech)**

Hope To See You There!

Thank you!



EPCH Contact Information:

-Gary Gray-HMIS Senior Administrator

ggray.epch@elp.twcbc.com

-Denver Herald- HMIS Support Technician

dherald.epch@elp.twcbc.com

-EPCH Phone Number (Office Hours: M-F 8am-5pm)

(915) 843-2170

WE ARE HERE TO HELP!