WEBINAR COMPANION

RHNTC
REPRODUCTIVE HEALTH
NATIONAL TRAINING CENTER

Data Protection is Everyone's Responsibility!

Do your part to protect your family planning project's information

The RHNTC presented a webinar entitled Data Protection is Everyone's Responsibility! on February 23, 2021. The following information includes the objectives, key definitions, risks to data protection, steps to take to minimize those risks, and resources covered during the 60-minute webinar. Access the archived webinar materials on rhntc.org.

As technology, workplaces, and family planning services and related data continue to evolve, the protection of organization and client information is critical. Family planning staff can take steps to protect themselves, their organizations, and sensitive data from cybersecurity threats. **Data protection is everyone's responsibility!**

Webinar Objectives

By the end of the webinar, participants are able to:

- Describe the importance of all family planning staff taking steps to protect against cybersecurity threats.
- Describe one or more steps an individual can take to protect the organization's data of all sorts (whether stored or shared).
- Identify one or more resources that can assist with additional data protection needs.

Key Definitions

- **Data protection:** Taking measures to secure electronic information stored on your computer, devices, network, and other accounts. Data protection includes the actions and processes that each person takes to protect private information.
- **Device:** Computer such as laptop, desktop, PC, or Mac; smartphone, or other things that conduct activities electronically, (e.g., "smart" TVs, coffee makers, or vacuums).
- **Operating system:** Manages all of the software and hardware on a device, coordinating to make sure each program running on the device gets what it needs (e.g., Windows).
- **Browser:** The software application on a device that is used to access the internet (e.g., Chrome, Safari, Firefox, or Edge).
- **Network:** All devices connected together through a central node. This can include local area networks where multiple devices can access each other, typically through WiFi or Ethernet cables.

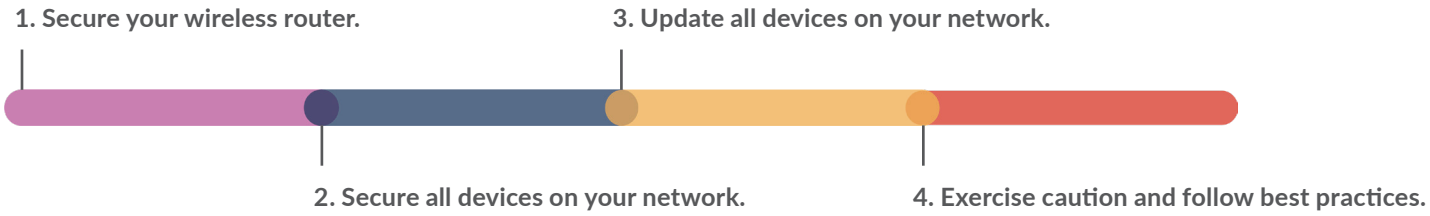
Importance of Data Protection

- People are increasingly working from nontraditional locations (e.g., their homes or in public spaces), which increases vulnerability and the risk of data exposure.
- Data collection and sharing have become increasingly granular.
- Regardless of data collection mechanisms (e.g., EHR, database, etc.), the need for security of storage and sharing remains.

The Risks

- **Ransomware:** A type of malware that takes control over a computer or computer system by encrypting all the data on the drive. The data are then held at ransom until a predetermined cost is paid.
- **Ransomware can be transmitted through:**
  - Emails posing as a legitimate business or tempting links
  - Trojans acting as update requests
  - Anti-virus programs patches and updates
  - False system updates
  - False "You've got a virus" notifications
  - Exploiting known network or security software vulnerabilities
- **Malware** can also result in theft of data and sensitive information without any signal that it has occurred. The sensitive information can then be revealed or sold.

Steps You Can Take to Protect Your Data



1. **Secure your wireless router.** Be sure the router software is up-to-date and password has been changed. Be sure the WPA2 data encryption is set as your security type.
2. **Secure all devices on your network.** Include work devices and any personal devices on your network. Change passwords at least every 90 days and use longer passwords. If your organization has a virtual private network (VPN), use that on your work device for stronger protection. If not, consider using your own VPN. Know your organization's data backup process.
3. **Update all devices on your network.** Be sure to include: Internet browsers, computer operating systems (e.g., Windows, Mac), smartphone operating systems, and other smart devices.
4. **Exercise caution and follow best practices.** Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source.
   - Try not to click links within messages. Instead, go to the site or account and log in. Confirm the information there.
   - Call or otherwise confirm with the sender before you click links in messages.
   - Look for consistency with communications you have previously received from the sender.

   Make good cyber choices!
   - Use a secure, encrypted connection like a VPN when communicating or accessing clinic or client data.
   - Make sure work devices are secured at all times.
   - Do not: use a personal email account to send or receive company emails, forward work emails to personal email accounts, send or share data through personal file-sharing tools, or discuss organizational matters through or on social media.

   Update your network password and then confirm with people around you that their devices and systems are up-to-date before sharing the new network password.

There is more to do!

- Develop strong organizational privacy and security policies and procedures.
- Ensue compliance with regulatory requirements like HIPAA.
- Plan for incident response.
- Ongoing training and support.

Resources

- Ransomware Guide: Best Practices and Response Checklist
- Ransomware: What It Is and What to Do About It
- Confronting Heightened Cybersecurity Threats Amid COVID-19
- How to Secure Your Home Wireless Network
- Cybersecurity Checklist for Staff Working Remotely
- Avoiding Social Engineering and Phishing Attacks
- Don't Wake Up to a Ransomware Attack

This publication was supported by the Office of Population Affairs (Grant FPTPA006030). The views expressed do not necessarily reflect the official policies of the Department of Health and Human Services; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.