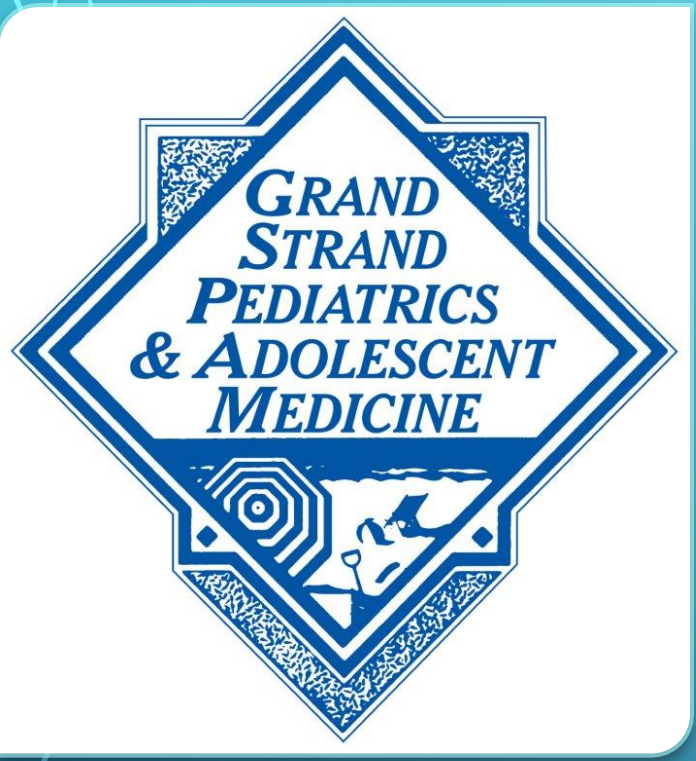


# QTIP LEARNING COLLABORATIVE- LESSONS LEARNED FROM RANSOMWARE ATTACKS

FEBRUARY 9, 2022

DANIEL SHULER, MD, FAAP

GRAND STRAND PEDIATRICS AND ADOLESCENT MEDICINE

# Disclosures:

- I am not an IT specialist.
- I am just a pediatrician with some decent “computer” knowledge who has been through this.
- Everyone else’s risk, experiences, and/or ”safety” is based on practice environment and possible corporate IT backup.

# First off: Ask questions about your current risk

- Ask of your EMR vendor, IT department, administration, network provider, IT specialists, etc.
- Depends on your EMR setup – web-based, cloud server, in house server
- Our mistake was doing this afterwards. Be pro-active. Ask now. Set up conference call/Zoom with all to discuss.

# Backup

- What type do you have?
- How is that used to get you back up running in the case of a ransomware attack?
- How long to get you restored completely from that back up?
- Is there a back up to the back up?
- Who is responsible for making sure the back up is running and complete? Is it automatic?
- Does it just back up EMR data or does it also back up server setup?

# Downtime procedures

- Does everybody know their “paper” jobs during downtime?
- Do you have readily available paper backup to document? Sick visit vs well visit sheets.
  Paper growth charts.
- Applies to other situations besides ransomware when your systems are down.
- Some staff and/or providers may have never documented on paper.
- Paper documentation of billing codes.

# Restoration procedures

- Who holds onto paper documentation until back up and running? Front staff, providers, clinical staff.
- Who is responsible for entering the information into the system? Shared vs just provider.
- Make sure everybody knows how to backdate timed information so that it is tied to the day of encounter, not when it is entered. Vitals, medication start date, etc. Depends on EMR setup.
- Timeline for entering information. Depends on how long that you are down.

# Restoration procedures

- What to do with paper documentation? Destroy vs scan in. Is it part of medical record or is it just notes to remember what you need to enter?
- Don't forget to have front staff to call and setup follow up appointments that could not be scheduled while you were down. Can cause headaches down the road. Make sure they keep a paper list.

# Prevention

- May be beyond the scope of this presentation. Again, I am not an IT specialist.
- Everybody's setup, practice type, hospital owned vs private practice affects where your risk may be.
- BUT I am told that something like 75% of ransomware comes from phishing attacks in emails.

# Prevention

- Review and update internet usage policy with all staff. What is allowed? Social media, private email, etc. How do you enforce? Asks your IT specialist about how to monitor or block access to certain sites.
- Services to educate and/or test your staff.

For example: knowbe4.com

# Questions?

- Again, I am not the specialist in this.
- Ask your "specialists" in that conference Call/Zoom meeting that you need to setup.