

NATCON21
FORWARD TOGETHER

***INFORMATION
TECHNOLOGY
READINESS***

INFORMATION TECHNOLOGY READINESS

ARE YOU READY FOR THE NEXT TECHNOLOGY CHALLENGE?

PRESENTER:

CHARLIE GRANTHAM

IT AND PROCESS OPTIMIZATION CONSULTANT

MTM SERVICES

CHARLIE.GRANTHAM@MTMSERVICES.ORG

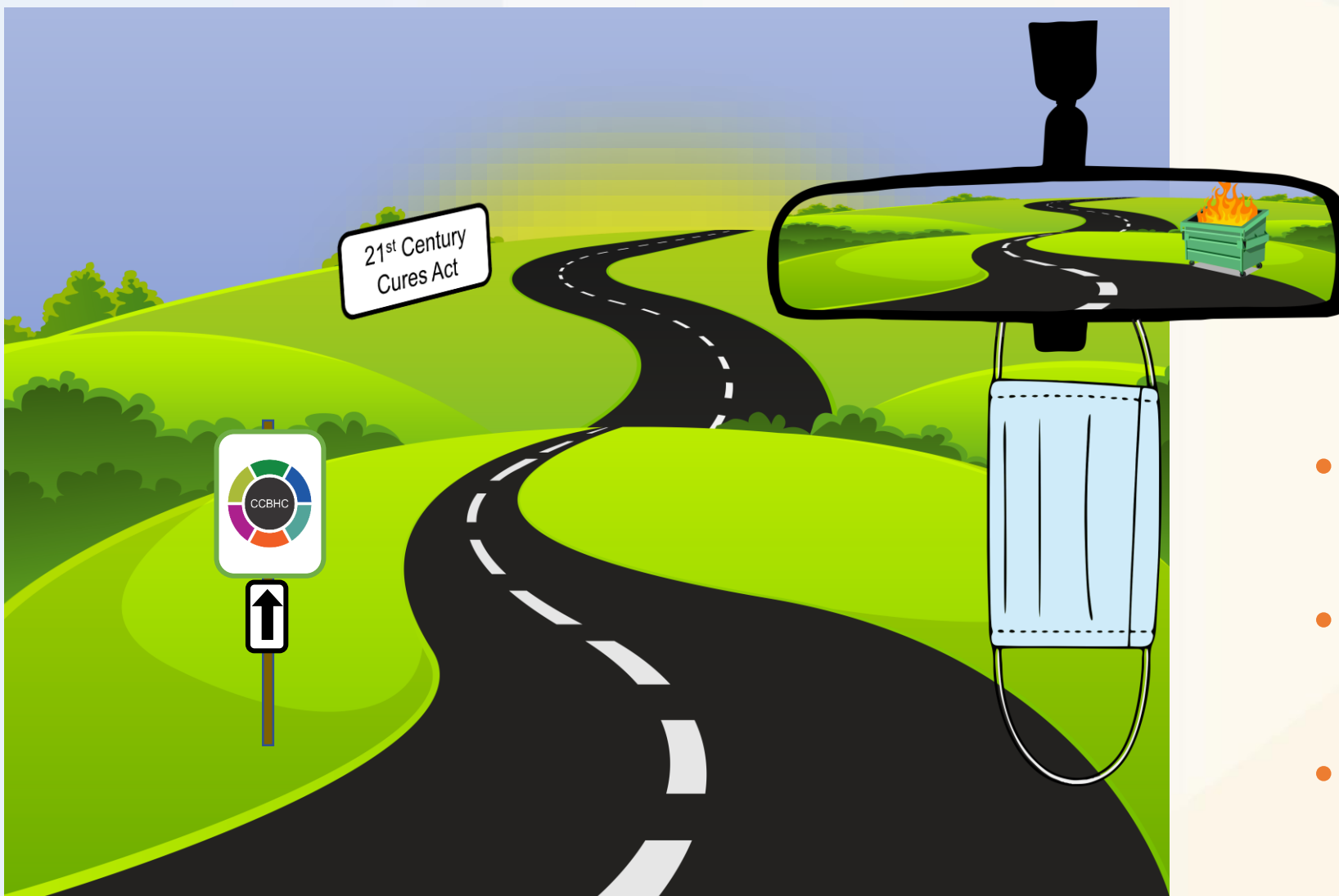
910-734-3141

WWW.MTMSERVICES.ORG



INFORMATION TECHNOLOGY READINESS

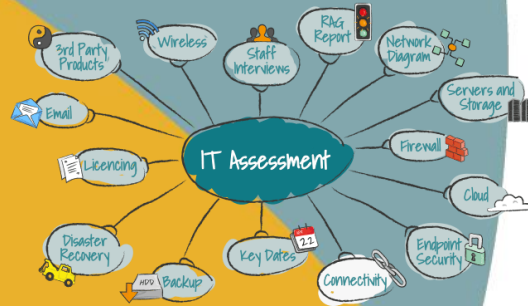
- CONSIDER WHERE YOU ARE NOW
- LESSONS FROM THE RECENT PAST
- BEING READY FOR THE FUTURE



CONSIDER WHERE YOU ARE NOW



TECHNICAL SYSTEMS



STAFF FACING SYSTEMS

STAFF SATISFACTION

6. Our Information Technology is robust and I rarely encounter system downtime.

Disagree Agree

14. Overall, how satisfied or dissatisfied are you with the Electronic Health Record?

Very Satisfied Somewhat satisfied Neither satisfied nor dissatisfied Somewhat dissatisfied Very dissatisfied

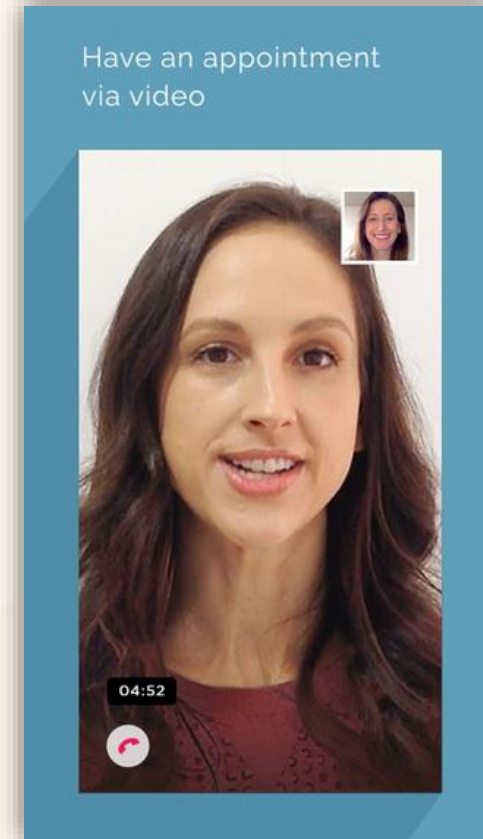
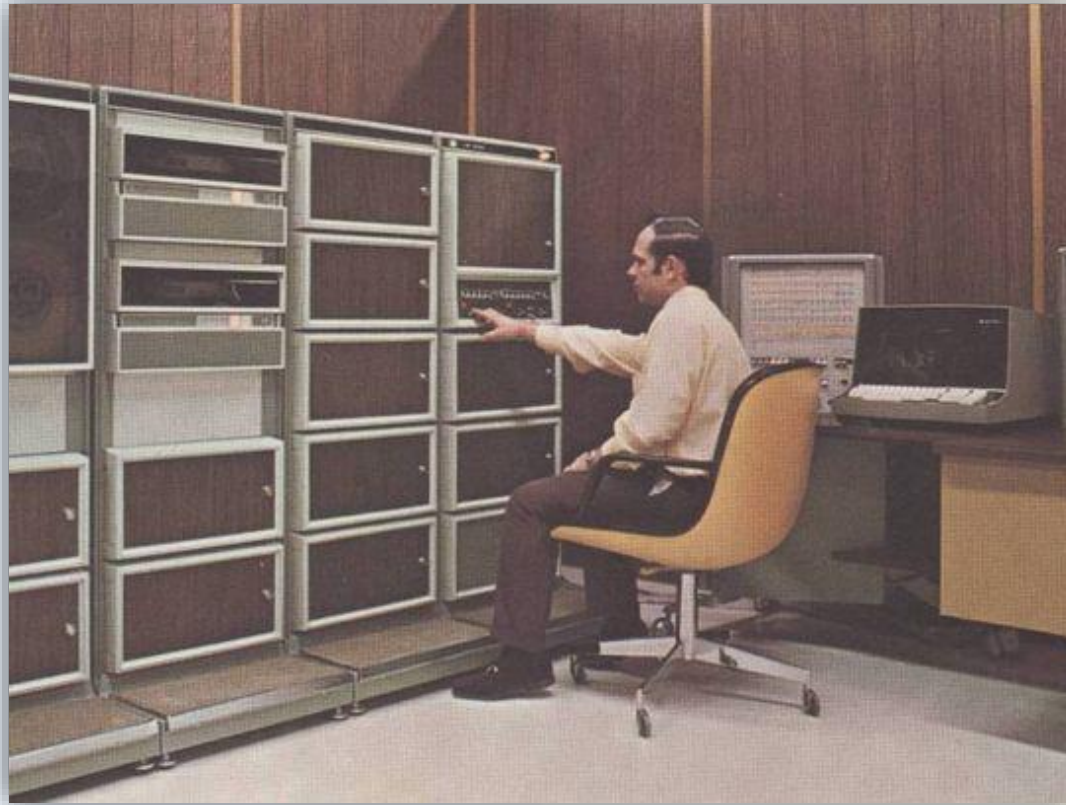


SECURITY

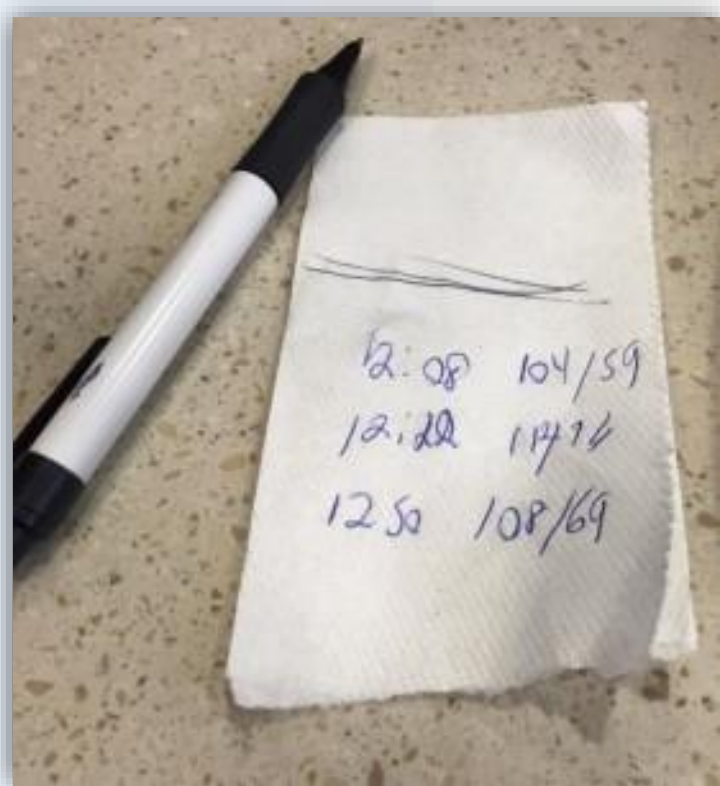


POLICY AND PROCEDURE

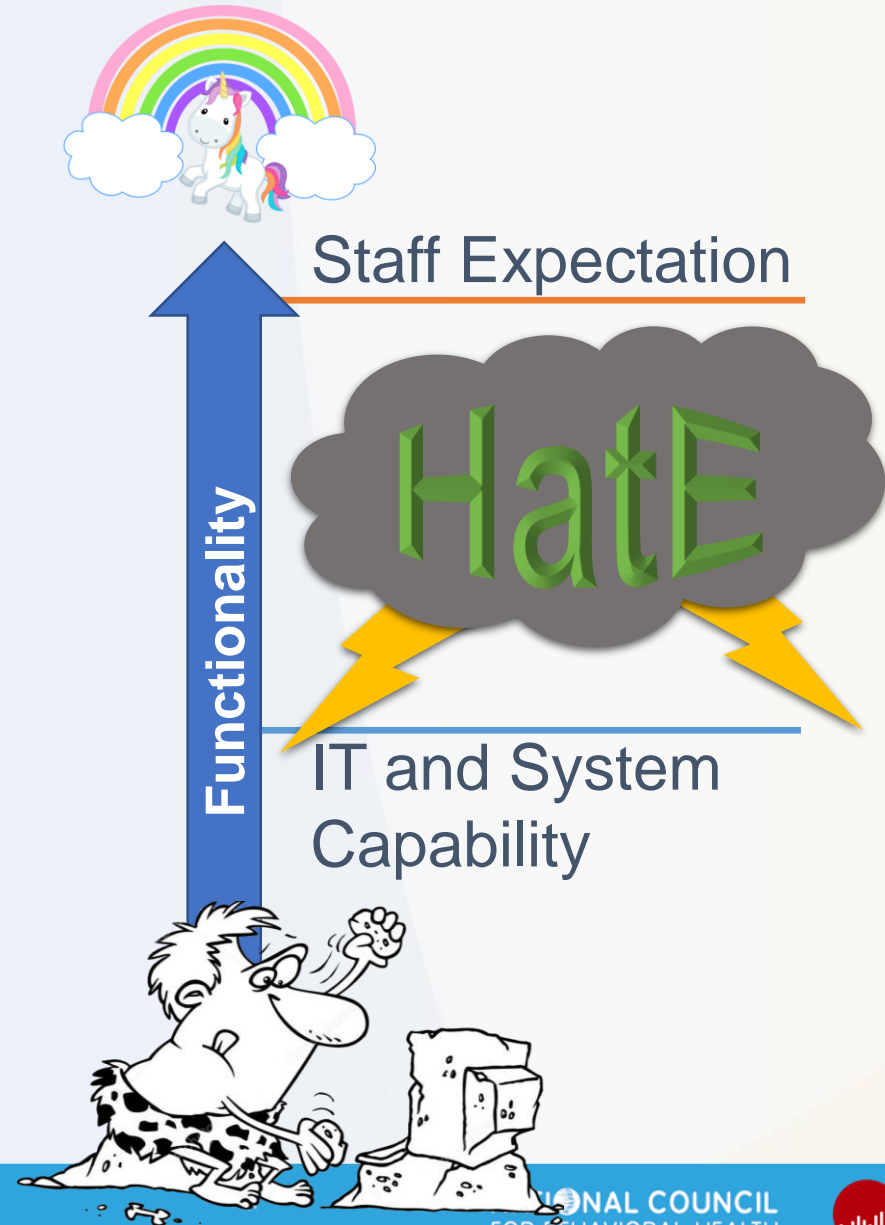
THE TECHNOLOGY WATERFRONT CAN BE WIDE



EVERY TECHNOLOGY IMPLEMENTATION IS DIFFERENT AND TAKES CONSTANT REFINEMENT



CREATING ALIGNMENT



Aligning
Expectations
with
Capability
is crucial.

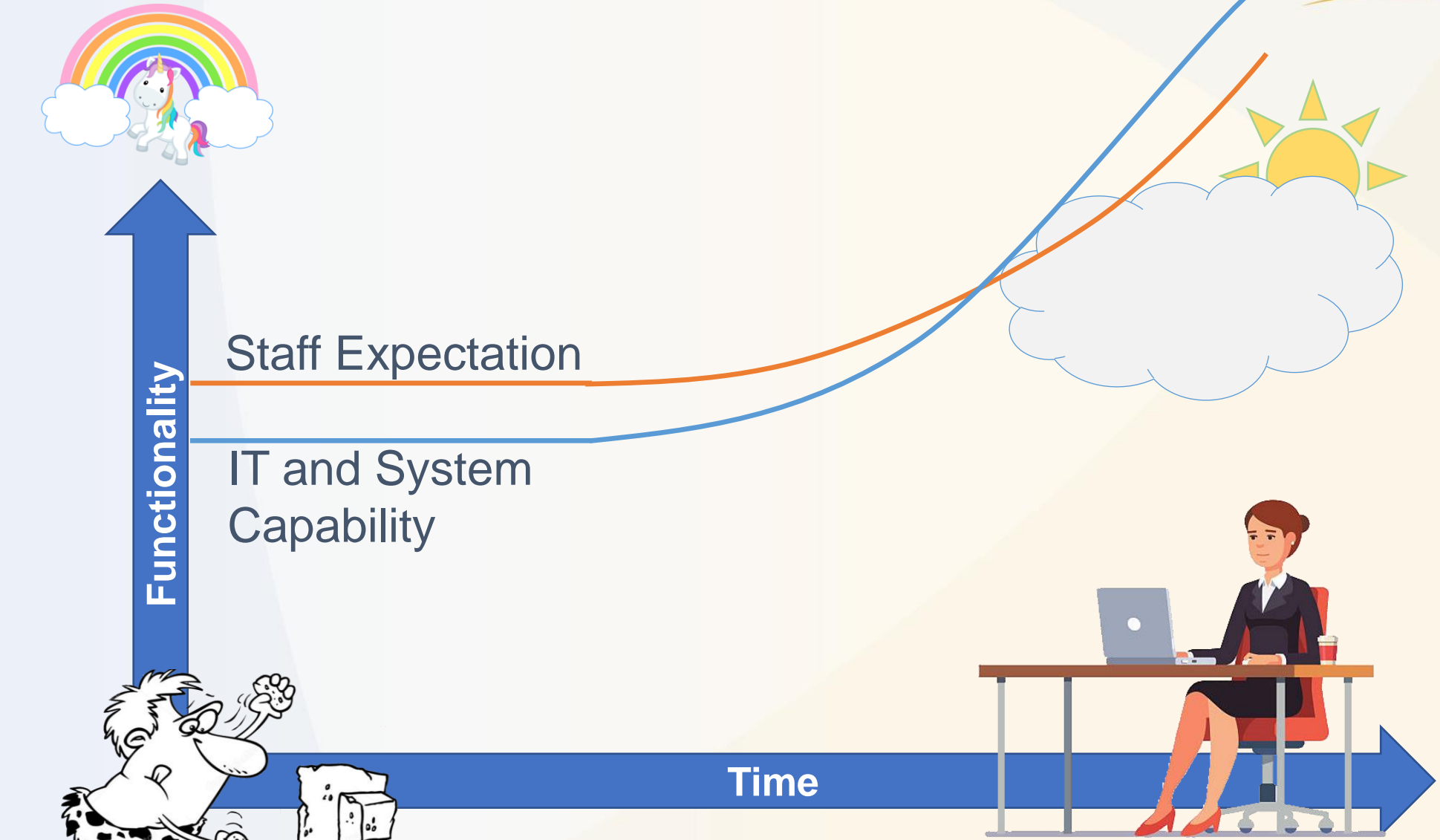
NO SHORTAGE OF DATA NEEDS



MEETING YOUR DATA NEEDS



CREATING ALIGNMENT



SECURITY

HEALTHCARE DATA'S CONSTANT COMPANION

- Desktop/Laptop Security
- Mobile Device Security
- Malware Protection
- Configuration Management
- Vulnerability Management
- Intrusion Protection and Prevention
- Password Management
- Access Control and Monitoring
- Remote Access and Authentication Control
- Physical and Environmental Security
- Secure Disposal

POLICIES AND PROCEDURES

- Information Security Policies
- Information Systems Policies
- Training and Awareness
- Business Continuity Management
- Auditing
- Downtime Policies for both Clinical and Technology areas



***Policy AND
PROCEDURE***

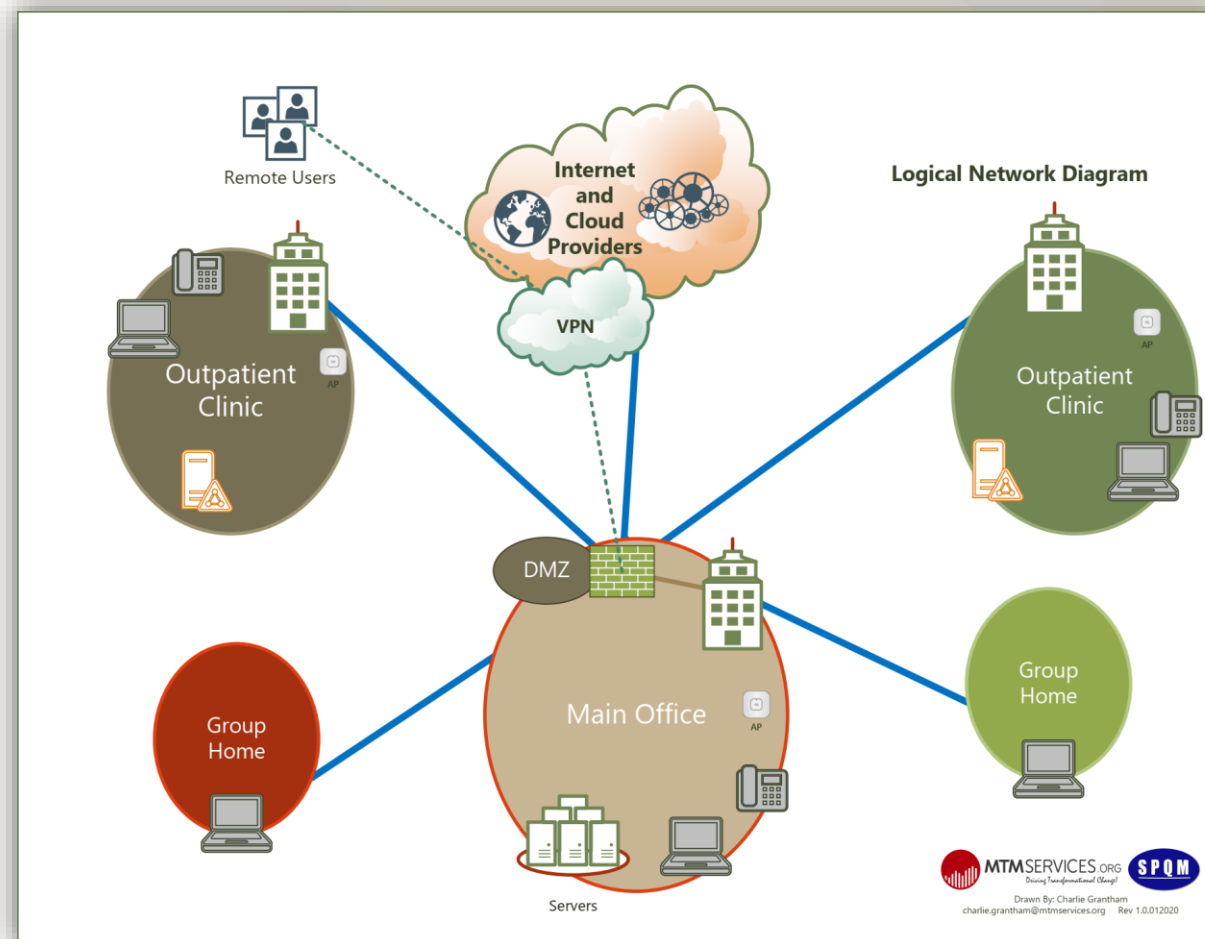
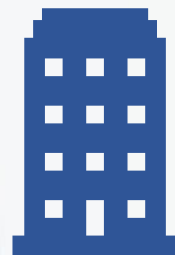
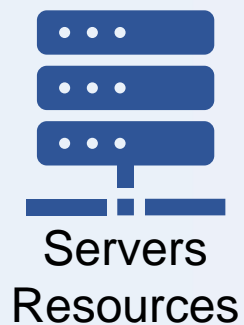
LESSONS FROM THE RECENT PAST

- Dispersed workforce adds additional complexity to the availability of Systems and Data
- Data use requirements can change
- Security and Quality Risks are ever present

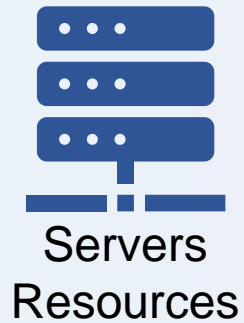


SYSTEM AVAILABILITY

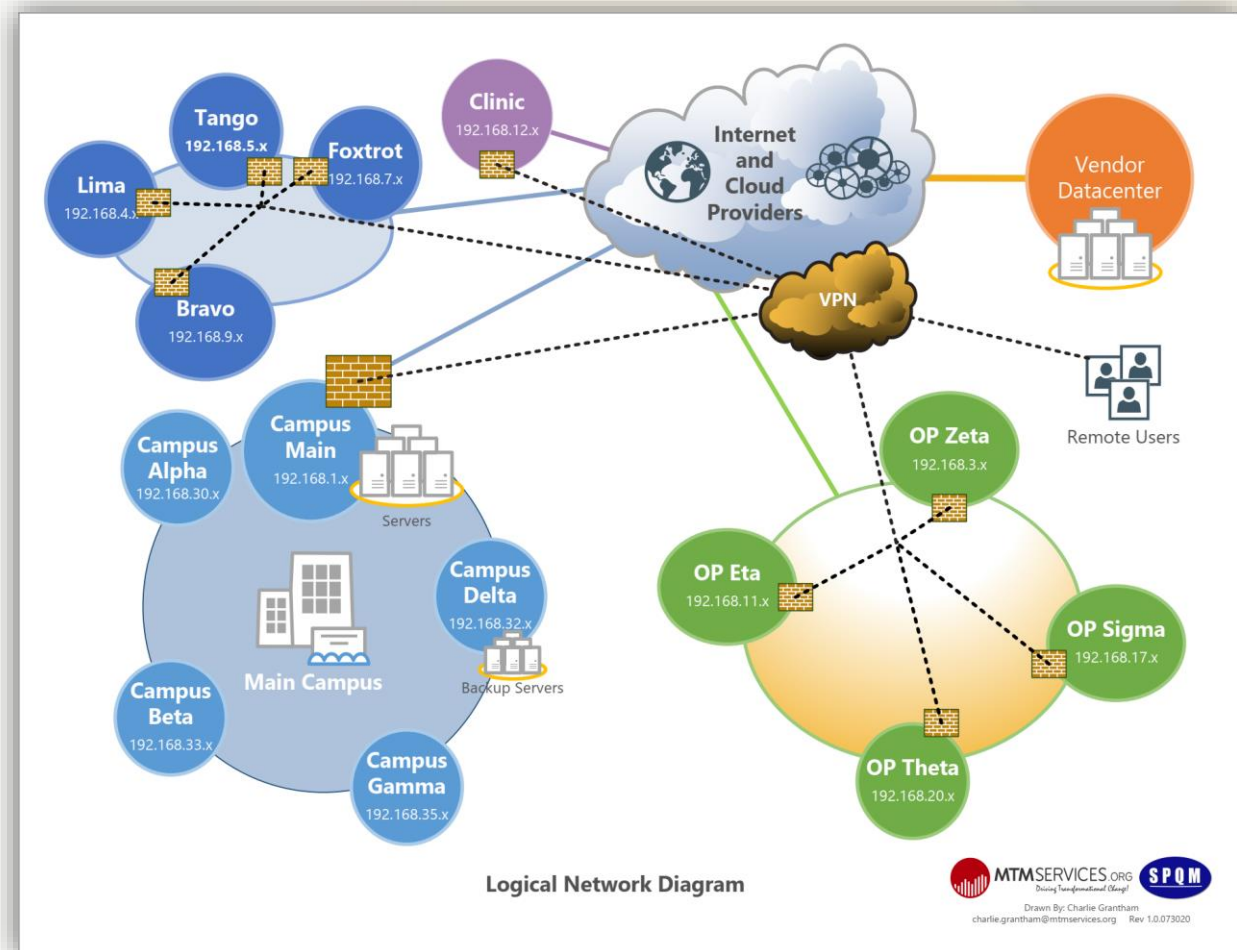
Pre-COVID with On Premises Systems



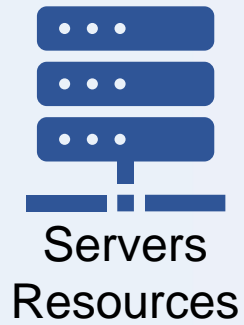
SYSTEM AVAILABILITY



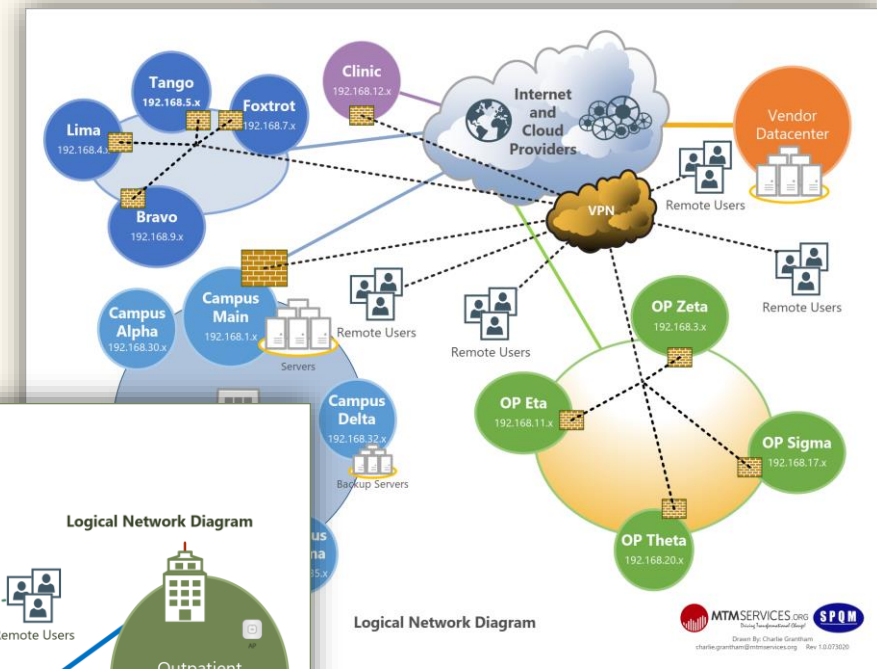
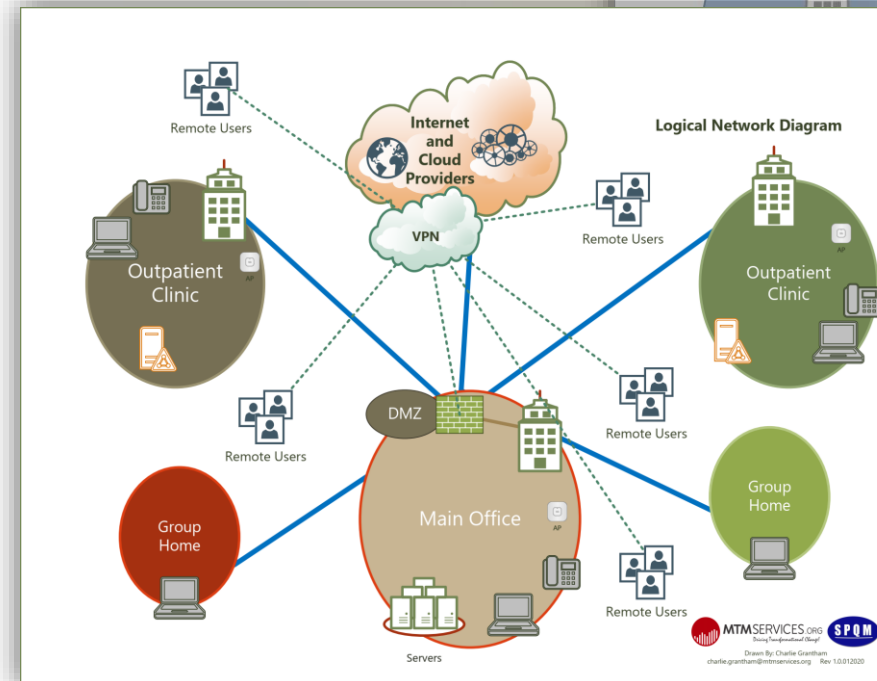
Pre-COVID with On Premises and Cloud Systems



SYSTEM AVAILABILITY

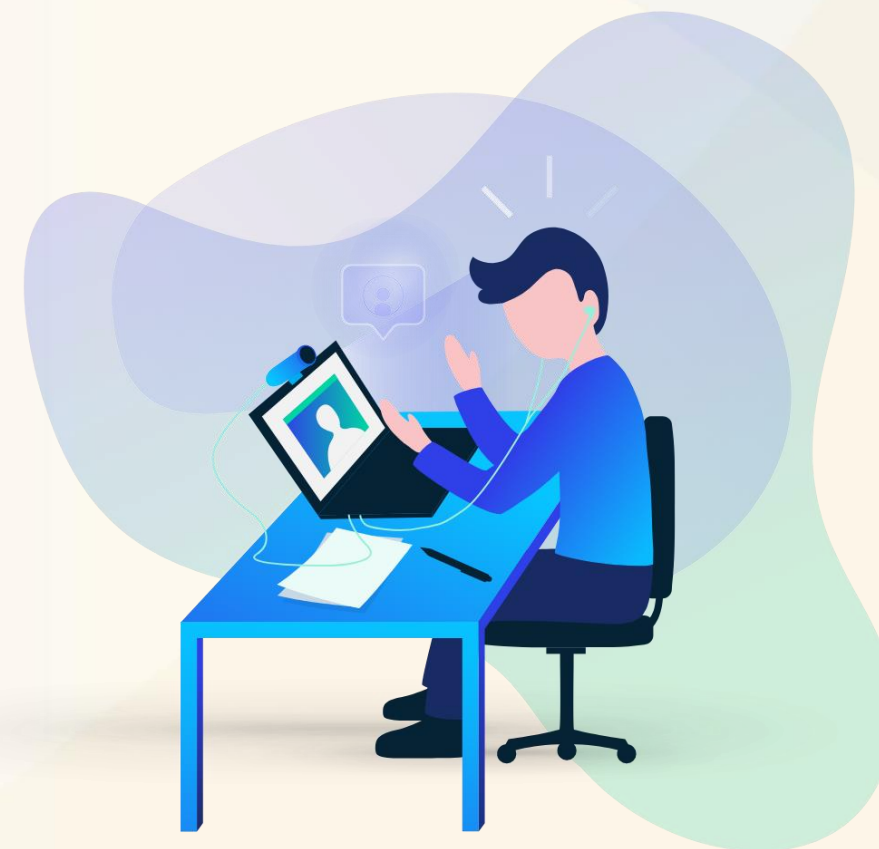


Post-COVID



DATA USE CHANGES

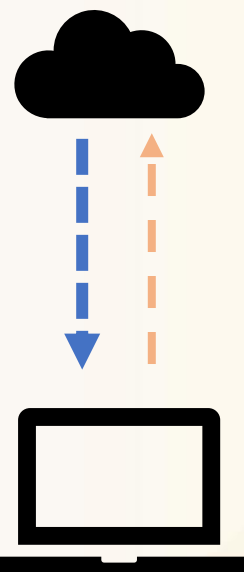
- Moving from primarily **consuming** data, to both **consuming** and **producing** digital content.



DATA USE CHANGES

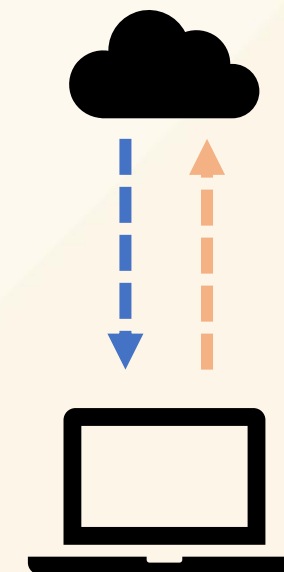
- Moving from primarily **consuming** data, to both **consuming** and **producing** digital content.
- **Asymmetric** vs. **Symmetric** data connections
 - One Telehealth video stream ~ 4 Mbit

Asymmetric



100 Mbit Download
10 Mbit Upload

Symmetric



400 Mbit Download
400 Mbit Upload

RISKS OF A DISPERSED WORKFORCE

More endpoints on more networks

- Increased risk of:
 - PHI/PHII Exposure
 - Introduction of malicious content
- Deploy Basic Safeguards:
 - Encryption
 - Removable Storage
 - Multi-Factor Authentication

Need for Quality and Oversight

- Setup “Norms” and codify with policy to insure a professional experience for your clients
- Use electronic systems to monitor and secure remote devices and users



BEING READY FOR THE FUTURE

Connectivity is key for all parts of the practice

- Work with your vendors to insure robust and redundant connectivity



BEING READY FOR THE FUTURE

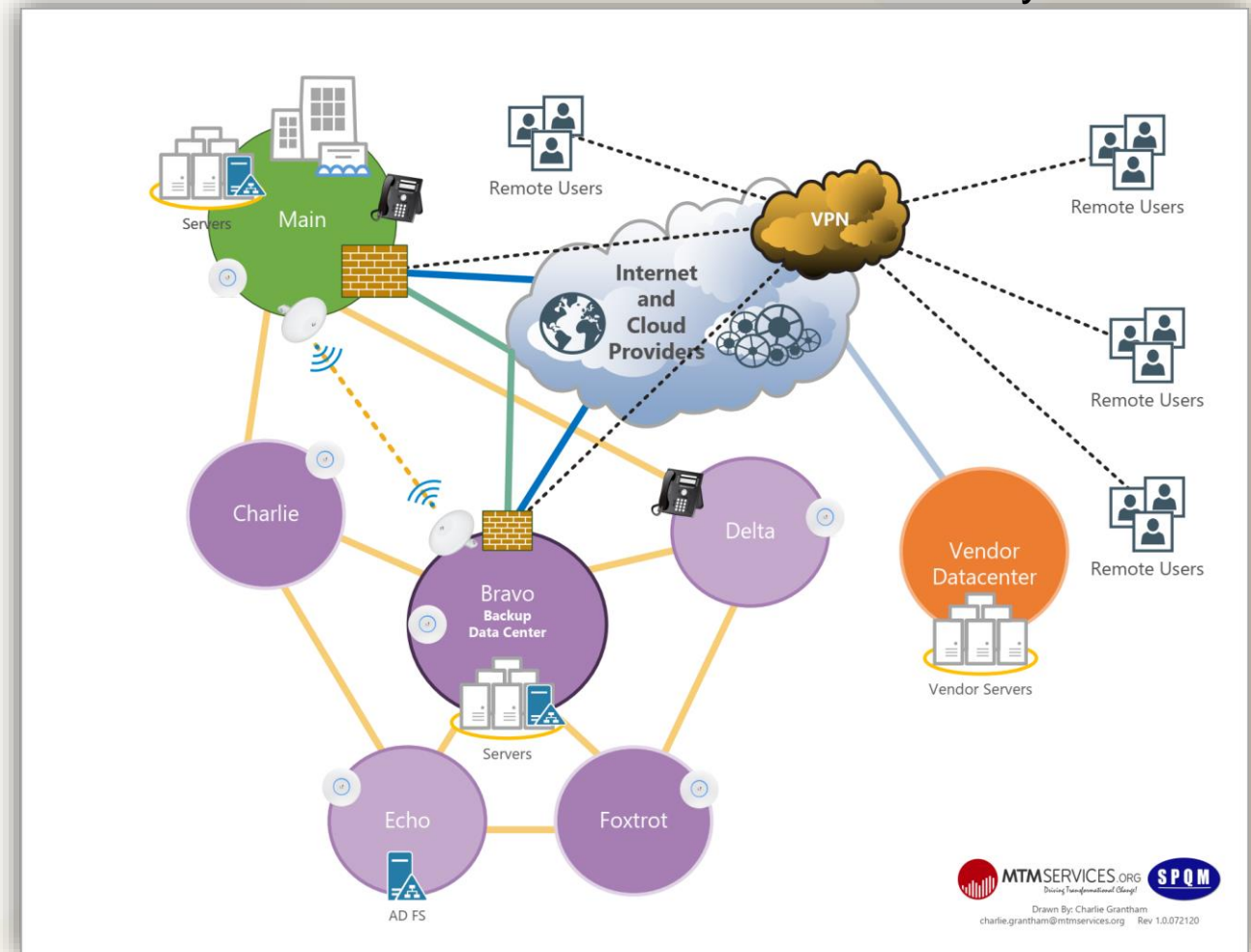
Post-Covid with Redundant Connectivity

Connectivity is key for all parts of the practice

- Work with your vendors to insure robust and redundant connectivity

Design networks to insure availability of local and internet resources

- Consider all forms of connectivity



BEING READY FOR THE FUTURE

Keeping Systems Secure with Technical Safeguards

- Passwords / Multi-factor
- Encryption
- PHI/PII Protections
- Centralized Management
- Auditing



1. West Virginia health center email breach exposes 3,700+ patients' info [Full story](#)

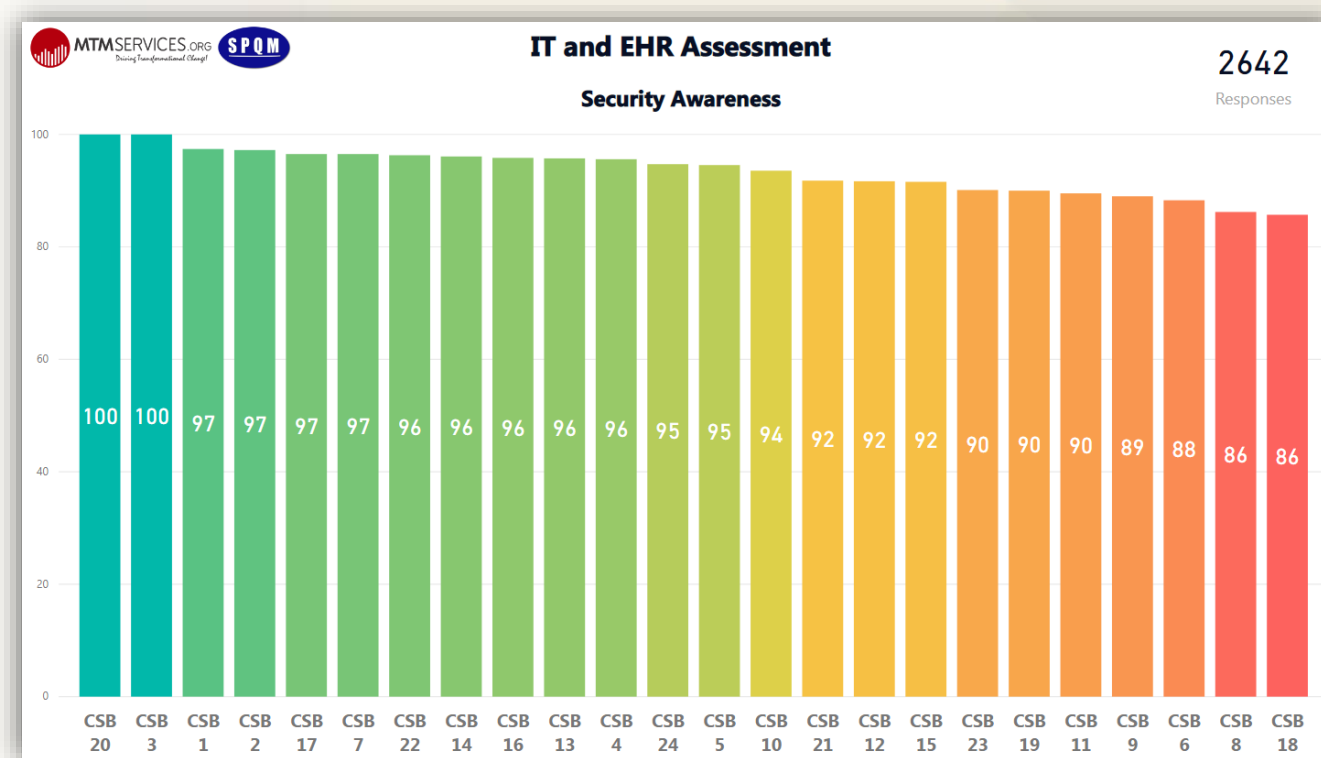
6. Alaska hospital getting a new EHR, says former employee snooped through files for 3 years [Full story](#)

8. Colorado health provider alerts 295,617 patients of data breach [Full story](#)

BEING READY FOR THE FUTURE

Data Security takes constant vigilance and reinforcement

- Create or buttress your Security Awareness Program
- Monthly HIPAA Walkthroughs
- Security Training at Orientation, along with additional “Online Learning/CE” required of all employees yearly
- Simulated phishing attacks
 - Follow-up training required for repeat offenders
- Mass emails warning about specific phishing attacks (including ransomware)



BEING READY FOR THE FUTURE

The use of Healthcare Data in the future...

- CCBHC's are data heavy and require specialized workflows to capture required data points
 - Knowledge of EHR system configuration and reporting are key
- The 21st Century Cures Act has changed data sharing from an Opt-In to and Opt-Out methodology.
 - Is your EHR vendor ready for that future?



BEING READY FOR THE FUTURE

- Value of additional training for Technical / Data / Clinical Staff
- No workflow too small or so large that it can't be improved
- With proper preparation, you **can** be ready for technology's next big challenge





NATCON21

FORWARD TOGETHER

Thank you!

CHARLIE GRANTHAM, MTM SERVICES

IT and Process Optimization Consultant

charlie.grantham@mtmservices.org

910-734-3141

www.mtmservices.org