MN Community MEASUREMENT

PIPE: Utilizing Advanced Healthcare Security

APRIL 16, 2024

Welcome!

Thanks for joining us today.

All webinar participants are in “listen-only” mode. To ask a question, please type your question into the “Q&A” box at the bottom of your screen at any time during the webinar.

MNCM will send a link to presentation slides and the recording to webinar attendees later this week.

MNCM PIPE Team

Will Muenchow
Vice President, Technology and Innovation

Lexie Adams
Data Quality Specialist

Elijah Gallenberg
Technical Project Specialist

Ellen Kormanik
Data Quality Supervisor

Maegi Yang
CHIRP Program Manager

Today's topic:

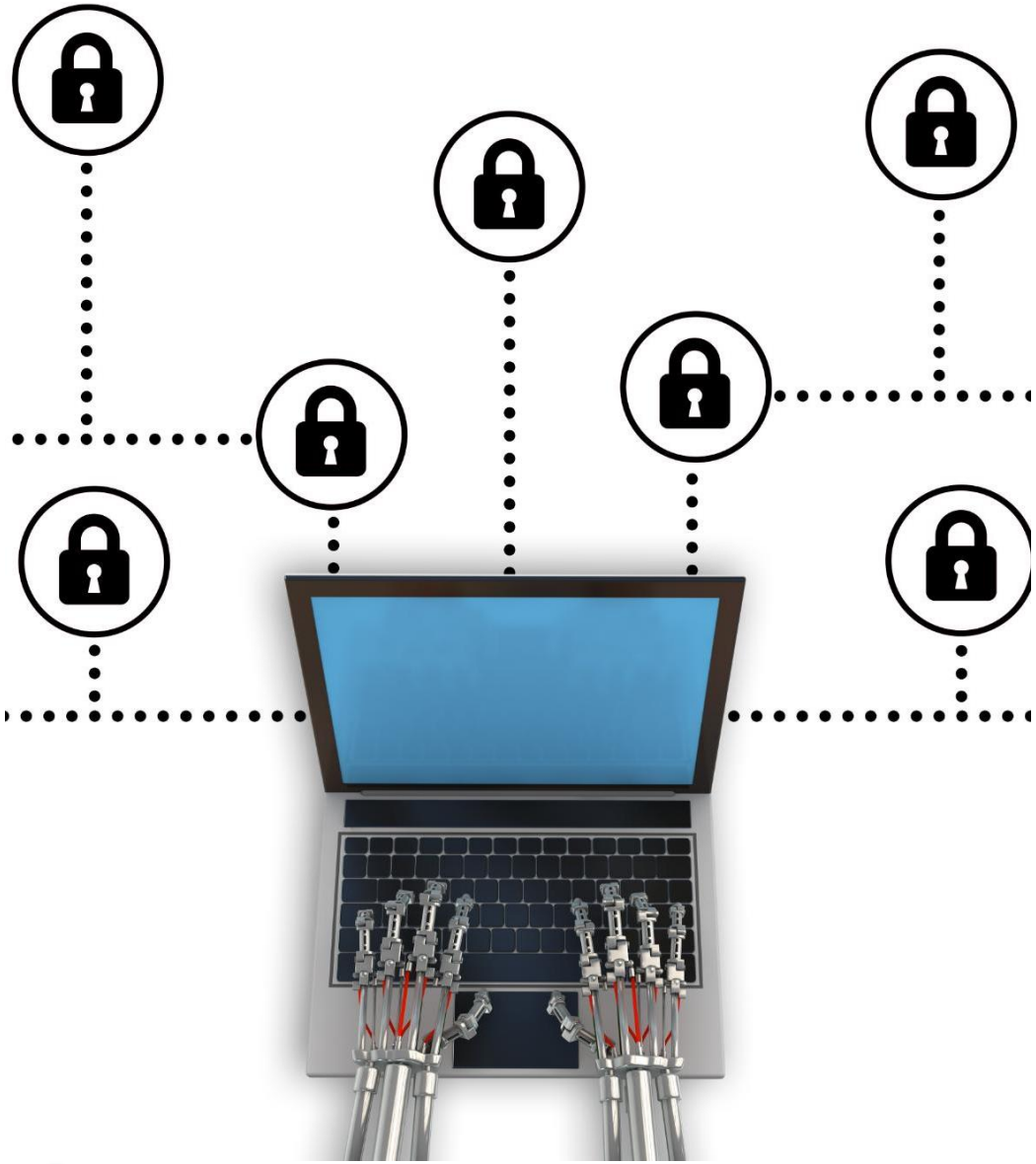
PIPE: Utilizing Advanced Healthcare Security

PIPE is MNCM's modernized approach to collecting data, calculating measures, and producing performance rates. We'll talk about:

- Password Requirements
- Muti-Factor Authentication
- Data Encryption (In Transit/At Rest)
- On-Going Application Security Hardening
- Account Auditing
- Annual Penetration Test
- Vulnerability Scanners & Management
- SOC2 Audit
- Summer 2024: MNCM Trust Page

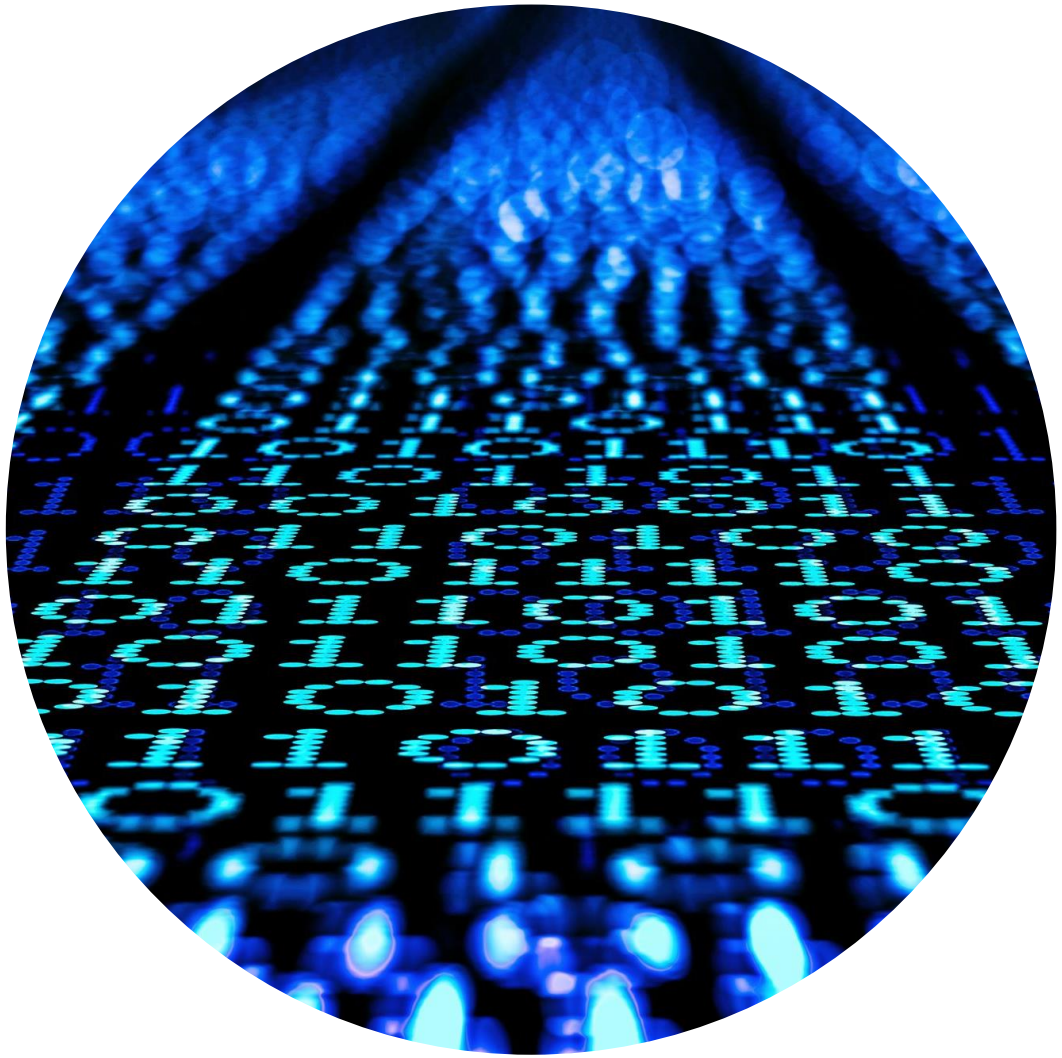
Password Requirements

- All passwords must be 16 characters or longer
- All passwords must contain at least one capital letter
- All passwords Must contain at least one non-standard character (!, @, etc.)
- Passwords must be changed every 90 days



Multi-Factor Authentication

- PIPE uses multi-factor authentication (MFA) to ensure that only authorized users can access sensitive data
- PIPE MFA requires users to enter a password and a unique code generated by PIPE and sent to the user through e-mail
- MFA makes it difficult for unauthorized users to access sensitive information
- Review of failed login attempts

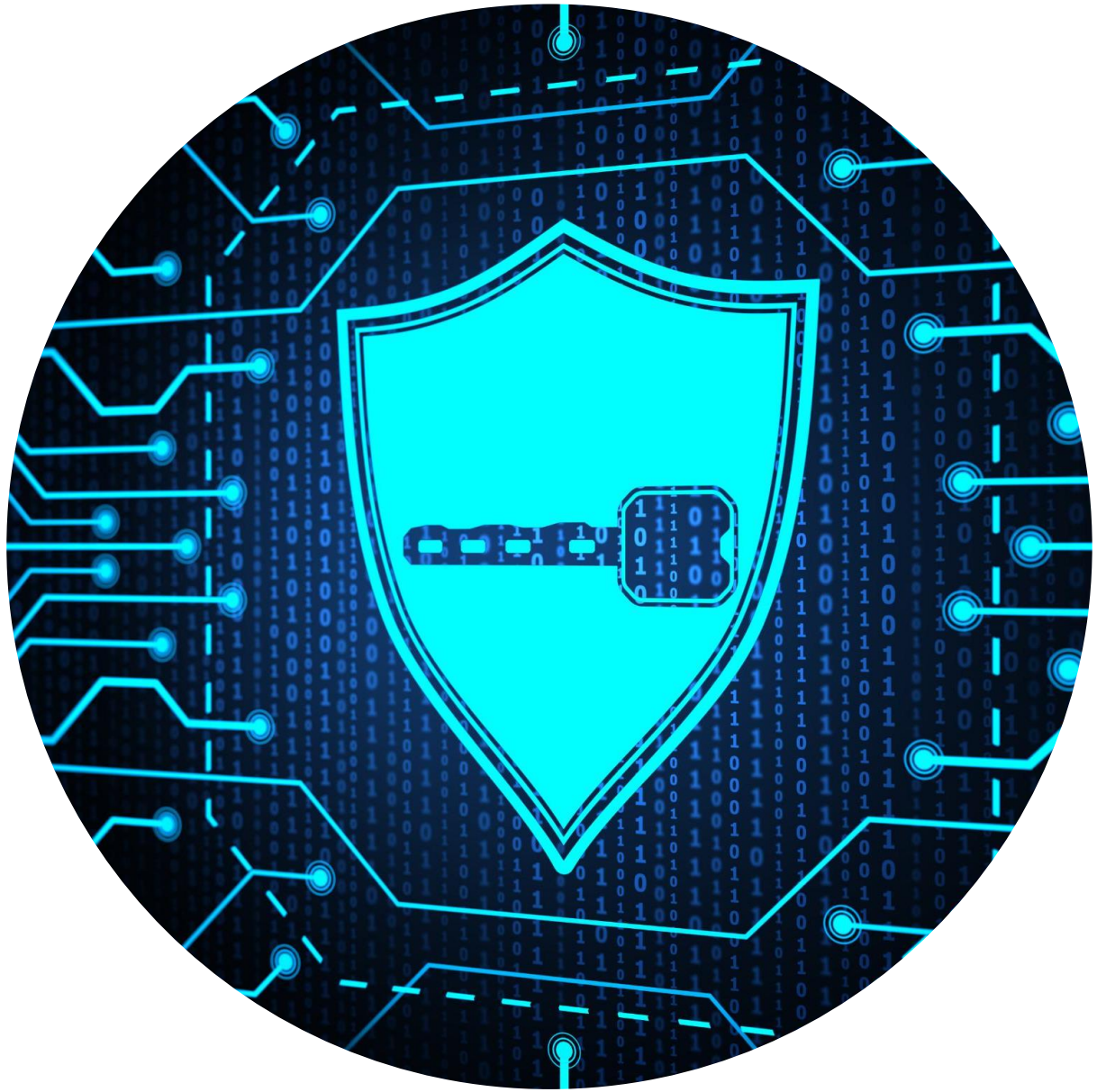


Encryption

- PIPE uses AES-256 to encrypt all user data
- AES-256 is a highly secure encryption standard used by the US Government
- Mandatory key rotation

On-Going Application Hardening

- Regular application updates improve security
- Security patches and software updates protect from vulnerabilities
- Internal application hardening provides additional security measures and is on-going (i.e. ZAP)

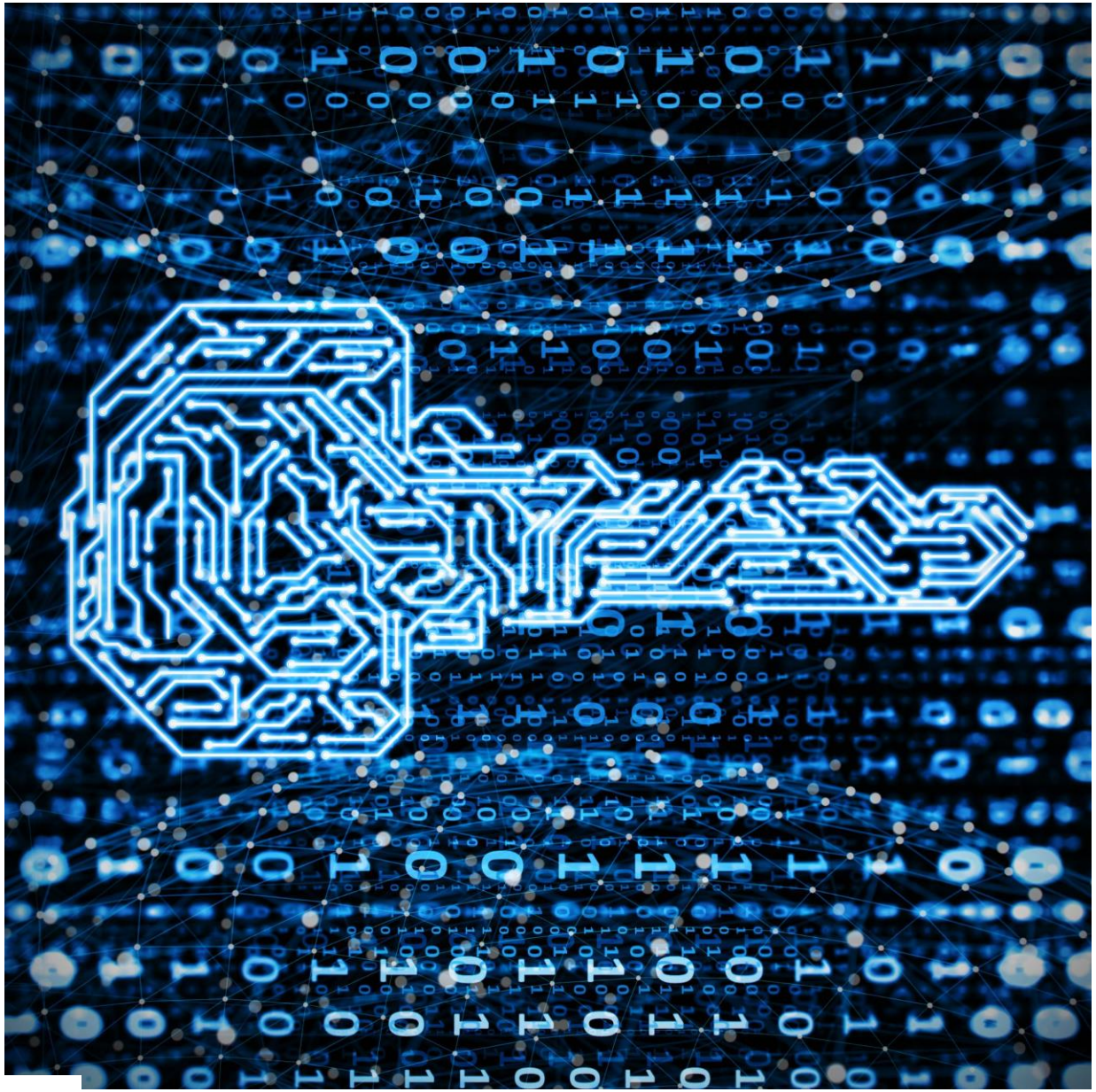


PIPE Account Audits

- MNCM regularly audits PIPE accounts for activity and use
- These audits ensure that only authorized users have access
- MNCM maintains logs on all access and termination request for PIPE

Independent Penetration Testing

- We use ethical hacker agencies to test our systems for vulnerabilities
- These hackers try to exploit our systems in the same way that real attackers would
- This allows us to identify and address vulnerabilities before they can be exploited by malicious actors



Vulnerability Management

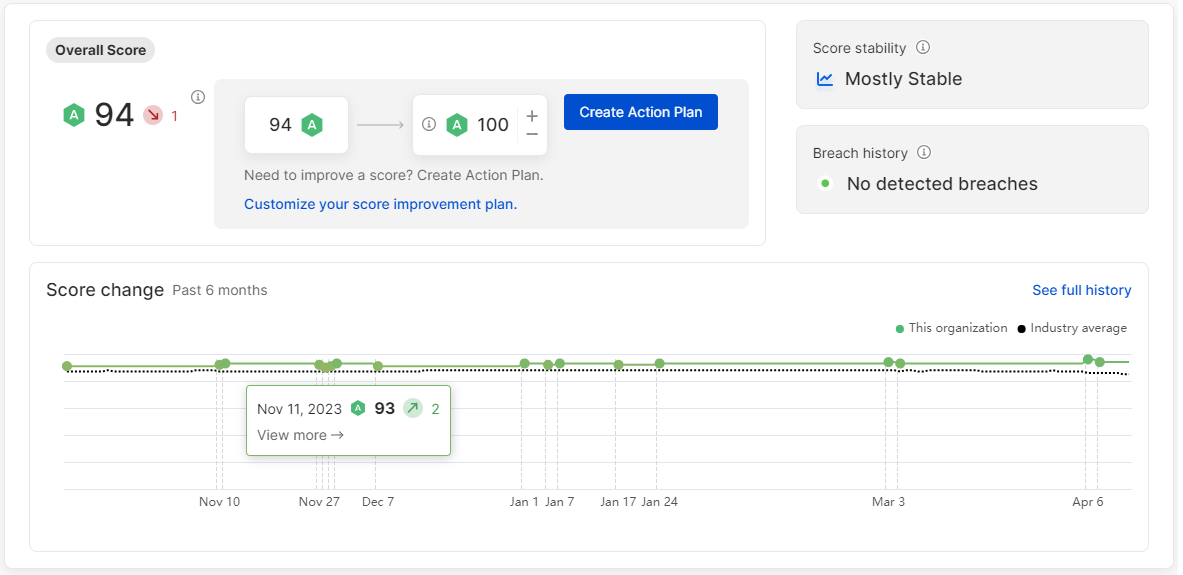
- PIPE uses advanced vulnerability scanning tools to identify and patch vulnerabilities.
- Risk-Based Prioritization
- Continuous Monitoring and Real-Time Insights
- Actionable Data and Reporting
- Our security team is always monitoring the latest threats and taking action to protect our users

SOC2 Audit

- SOC2 is an auditing procedure that ensures service providers securely manage data to protect the interests of their customers and the privacy of their data
- SOC 2 compliance is based on the Trust Service Criteria which include five areas: security, availability, processing integrity, confidentiality, and privacy
- SOC2 audits are performed by independent auditors who evaluate the design and operating effectiveness of a service provider's controls
- All MNCM data system are hosted on SOC2 Type2 audited environments.
- MNCM is currently in pre-audit SOC2 and will begin our SOC2 audit in May, 2024.

MNCM Trust

- The MNCM Trust Page is where users can find information about the security and privacy of MNCM and PIPE
- It will include details about audits, pen test reports, and other relevant information for PIPE users and organization
- The page will also include results from on-going independent audits like securityscorecard.com and others



Office Hours Schedule

Schedule	
Date	**Office Hours Topic**
4/9/2024	**Pre-implementation step: readiness assessment, timeline & what to expect during onboarding**
4/16/2024	**Security- guest speaker Will Muenchow**
4/23/2024	**Data file extract guidance**
4/30/2024	Encounter file * tentative
5/7/2024	TBD
5/14/2024	TBD
5/21/2024	TBD
5/28/2024	TBD
6/4/2024	TBD
6/11/2024	TBD
6/18/2024	TBD
6/25/2024	TBD
7/2/2024	TBD
7/9/2024	TBD
7/16/2024	TBD
7/23/2024	TBD
7/30/2024	TBD
8/6/2024	TBD
8/13/2024	TBD
8/20/2024	TBD
8/27/2024	TBD
9/3/2024	TBD
9/10/2024	Registration only**

*= Tentative office hours topic. All topics will be confirmed at least 2-weeks prior to the scheduled meeting. Topics in bold have been finalized. Office hours will be recorded and will be available to onboarding groups.

**Registration only will be an hour-long session and will walk through the PIPE portal, the PIPE provider file and what is different from DDS registration

***Next Up:** Elijah Gallenberg discussing Data File Extract Guidance

https://helpdesk.mncm.org/helpdesk/KB/View/70868148-

Q&A/Discussion

Please type your questions into the “Q&A” box at the bottom of your screen

Thank you!

To learn more about PIPE:

- Email support@mncm.org with additional questions