MOBILE DEVICE MANAGEMENT (MDM)

OSTRA
CYBERSECURITY

MDM is...

- A solution for protecting corporate data stored in mobile devices (phones/tablets)
- A method of controlling access to corporate data through virtual isolation (containerization)
- A complement to third-party apps to assist in compliance of PHI/PII handling

MDM can...

- Isolate business mobile apps (e.g., O365, CRM, productivity)
- Remotely perform factory resets on company-owned phones and tablets
- Push applications and best practice security policies (e.g., enforce password requirements, limit functionality)

MDM would best suit clients...

- Who manage company-owned mobile devices and want to limit employee access to business applications
- Who allow the use of personally-owned mobile devices for accessing business applications
- Who need a new way to prevent unauthorized access and intentional loss of corporate data

MDM cannot...

- Secure text messaging, photo apps, or other native applications to meet HIPAA compliance
- Act as an anti-virus or malware detection software, which is covered by regular OS patching on the device
- Containerize entire phone or tablet (only apps available from the app store and added to the portal)

Questions? Contact us at support@ostra.net