Velaris Medical Centre

VelTech Data Hacking and Ransom Timeline

Timeline

- Alerted, June 21, 2018 at 10: 45 a.m. of the VelTech medical data computer system breach with the message, “Attention Velaris Medical Centre, we now have control of your computer systems. In order for us to go away, you will need to deposit 10,000,000 Bitcoins to this address: 456789092zzz.muney.111.”
- Standardized message was hospital wide and extended to Velaris Medical Clinics and Pharmacies.
- Notified the local medical compliance officer by 10:55 a.m., along with the FBI, and the regulatory HIPAA agency.
- Limited hacker access by 11:07 a.m.
- Established a secured data alert system at 11:15 a.m. and established the Data Crisis Helpline at 11:20 a.m.
- Shut down the MyVelaris Patient Portal access, at 11:30 a.m., and this was decided by Carol Smith, Health Information Manager, and Sam Paul, Medical Director.
- Decision to move critical care patients, was made at 11:30 by Sam Paul.
- Began transferring critical care patients at 11:45 a.m. and all incoming EMS were notified to reroute to St. Clair Hospital.
- Joined by FBI IT agents at 1:27 p.m.
- Contained the system hacking at 2:45 p.m.
- Determined the source of the hacking was Terrance Bones. The IP addressed was traced to a Starbucks near Portland, OR.
- Secured and resolved the situation by 3:05 p.m., which allowed all of Velaris Medical Centre, Velaris Medical Clinics and
  Pharmacies to run normally.
- Launched a new security system at 3:30 p.m., as part of the VMC IT Department collaboration with FBI IT specialists.
- Reopened MyVelaris at 4:00 p.m.
- Announced the, all-clear, at 4:30 p.m. for all systems to function normally.