



Security at Progressive Medical, Inc.

Angelo Mazzocco
Chief Information Officer



May 2009

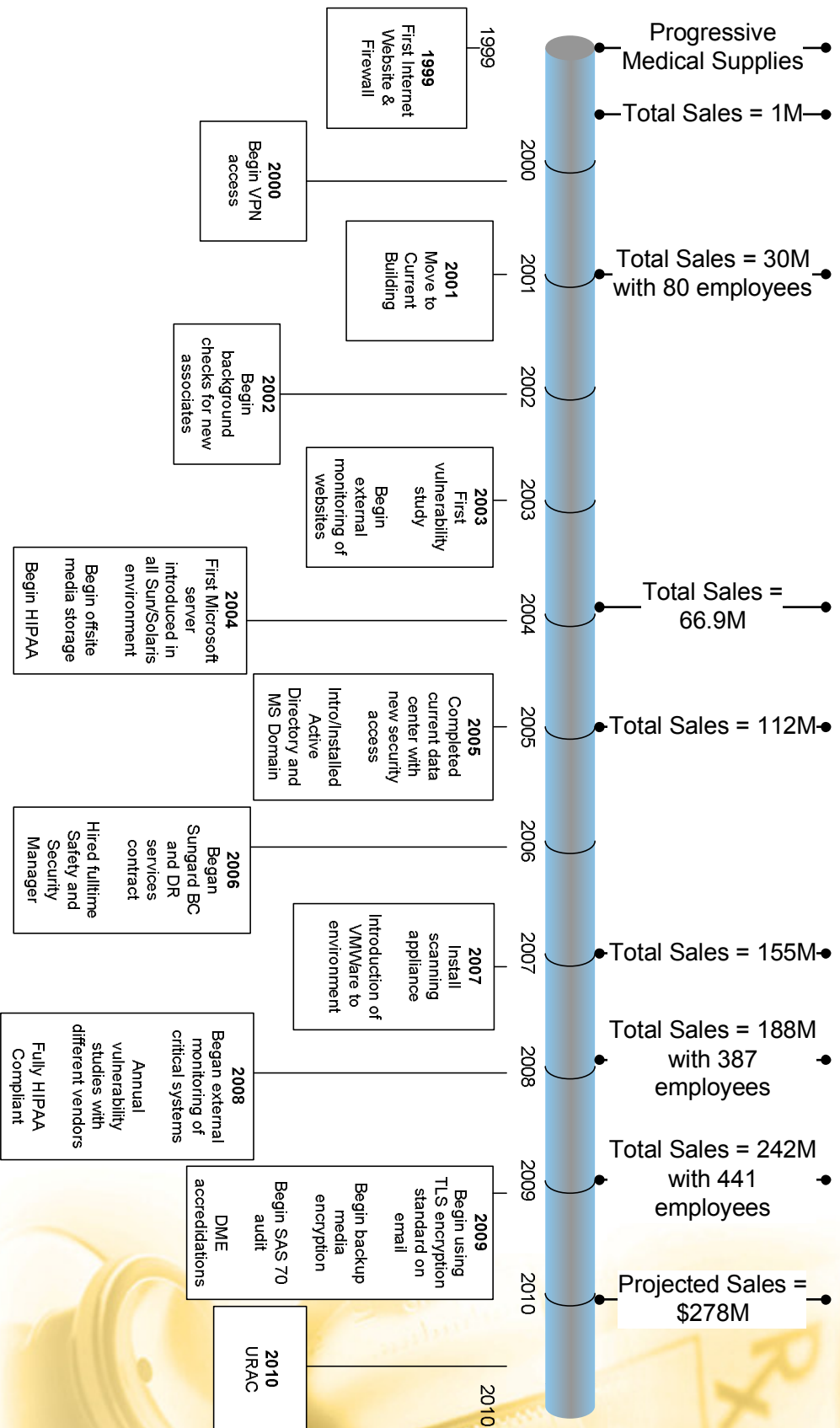
Continually exceeding expectations

PROGRESSIVE
Medical, Inc.

Who is Progressive Medical?

Progressive Medical, through a national network, offers cost containment services and products to the managed care industry. One call to Progressive Medical is all it takes for the case manager to be assured that their eligible injured party is receiving the best care, services, medication and equipment necessary to aid in their recovery.

Timeline



Continually exceeding expectations



Security

- Security as a Foundation
 - Confidentiality
 - Integrity
 - Availability

Sources

Hack Proofing by Huston, et al.

IT Policies and Procedures by Jenkins and Wallace

CIO Forum of Central Ohio

Security Policy

- Policy Regarding Information Security Policy
 - Policy Exceptions
 - Policy Reviews
 - Policy Change Management
 - Policy Enforcement
 - Policy Awareness
- Internet Use
 - General Internet use
 - Email
 - Blogs
 - Instant Messaging
 - Twitter, Yammer, Microsoft Communicator



Security Policy

- General Computer Usage
 - Non-Progressive Medical owned computer and network hardware and software
 - Intellectual property rights (including software licensing, music, video, etc.)
 - Circumventing security
 - Hacking or testing Progressive Medical security
 - Data retention and destruction
 - Mobile storage
 - Workstation security (desktops and laptops)

Security Policy

- Networks
 - Wireless
 - New Network connections
 - Changes to connections
 - Discontinuing connections
 - Safe and sane network protocols
 - Firewalls
 - Remote Network Access
 - Privileged Remote Access



Security Policy

- Physical security (of information and computing resources)
 - Environmental controls (fire, HVAC, etc.)
 - Doors
 - Windows
 - Clean desk
 - Highly secure areas
 - ID badges
 - Laptop and mobile devices



Security Policy

- Detection – Logging, Monitoring and Reporting
 - Logging
 - Off-box logging
 - Log record retention
 - Reviewing logs
 - Reporting incidents
- Response
 - Backups
 - Offsite storage
 - Planning
 - Testing



Security Policy

- Personnel
 - Roles & responsibilities
 - Awareness training
 - Terminations
 - Job changes
 - Monitoring and the right to search
- Encryption
 - Acceptable cryptographic methods
 - Unauthorized use of encryption
 - Encryption keys
 - Key escrow



Security Policy

- Technology Development and Maintenance
 - Segregation of duties
 - System configurations
 - Change management
 - Vulnerability management
 - Anti-virus and anti-spyware
 - Secure applications
 - Development environments



11

Security Policy

- Access Management
 - User accounts
 - Password sharing
 - Password encryption
 - Access privileges
 - Outsourcing and 3rd parties



Security Policy

- Data Classification
 - Roles and Responsibilities
 - Protecting Public Information from illicit viewing/access
 - Protecting Internal use Only (IUO) from illicit viewing/access
 - Protecting Confidential information from illicit viewing/access
 - Protecting Confidential & Sensitive information from illicit viewing/access

Questions??

