Paul Connelly, Hospital Corporation of America

- **HCA**
  - 163 hospitals, 109 freestanding surgery centers, 700 physician practices, and 199,000 employees
  - Approximately 5% of health care provided in the US
  - Provide outsourced IT to approximately 100 non-HCA hospitals
- **Culture**
  - Quality of care
  - Compliance
    - Security
- **The Perfect Storm of risk we face**—
  - Growing volume and value of information we handle
  - Growing distribution, access, and communication requirements for this data
  - Growing impacts from losses of this data
  - Growing threats to this data
Work-arounds we see that lead to security risks

- **Physical**
  - Access doors
  - IT closets
  - Vendor access
- **Network**
  - Bypassing access controls
    - Password sharing
    - Controls over physician office staff access
    - Inappropriate access
  - Going outside our network
    - Use of personal cell phone to text patient info to physicians
    - Use of Guest Internet access to use personal Gmail, DropBox, and cloud-based collaboration sites to exchange data
  - New products
- **Data**
  - Use of USB drives, DropBox and external collaboration apps
  - Use of personal devices
Key challenges that lead to work-arounds

• Need for speed: Clinicians are the worst offenders, not because they are bad people, but because speed and focus on patients is king
  – We want their focus to be on patients; the goal for us is to make security invisible or automatic
    • Integration of applications
    • SSO, Tap&Go
    • Automated account provisioning/de-provisioning based on role from credentialing

• Technology:
  – Hospital technology not keeping up with consumer technology people use every day
  – Medical devices usually have no security built in, and bolt-ons are viewed as obstacles
  – Poor interoperability between devices

• Lack of consistency: Security standards vary wildly between hospitals