4sighthealth
imagine better healthcare

Big Data's Ups and Downs:

The Good, The Scary and The Creepy

February 10, 2016

Big Data's Ups and Downs:

The Good, The Scary and The Creepy

By David Johnson, CEO

Big data analytics are essential for understanding consumer preferences. Collecting, measuring and evaluating consumer data drive strategic growth and customer acquisition. Companies use big data to design appealing marketing campaigns to sell products and services.

Having the right data at the right time is essential for advancing value-based care delivery and engaging customers. Integrating big data into operations will revolutionize healthcare service delivery, business models and consumer outreach. Buckle up.

Big data has good, scary and even creepy applications. Three front-line stories illustrate the range of big data's expanding impact.

The Good: Analytics-Boosted Performance

After finishing a distant 10th at the World Championships in 2012, the U.S. women's cycling knew they had to improve their performance to compete for medals at the upcoming London Olympics. The struggling team turned to former Olympian cyclist Sky Christopherson. Disgusted with cycling's doping culture, Christopherson had developed an analytics-based training programed named "Optimized Athlete." His mantra was "data not drugs."

In the three months leading up to the Games, team members became big data repositories. Computers analyzed reams of nutrition, endurance, bio-physical, environmental and micro-performance measures. Small adjustments turbo-charged individual performance. Here's an example:

"…one cyclist, Jenny Reed, performed much better in training if she had slept at a lower temperature the night before. So she was provided with a temperature water-cooled mattress to keep her body at an exact temperature throughout the night. This had the effect of giving her better deep sleep, which is when the body releases human growth hormones and testosterone naturally…"

Big data analytics turbo-charged "precision" training by quantifying factors that influence performance. These factors included training loads, endurance recovery cycles and muscle regeneration patterns. The program also sensed stresses and minimized injuries. The data eliminated guesswork and primed the athletes for peak performance. They were ready for London.

Training hard and smart with data-driven performance adjustments propelled the U.S. women's cycling team to Olympic glory. Surprising the cycling world, the U.S. team captured the silver medal. Big data geeks around the world celebrated with the victorious U.S. women

The Scary: Healthcare's Ominous Cyber Threat

Healthcare is a "target-rich" environment for cyber criminals. Digitized data passing through cyber-space invites "unwanted guests." According to the New York Times, there were 750 major breaches at healthcare organizations from 2010 – 2015 affecting 29 million people.

Attacks on Anthem and Premera insurance providers compromised personal information of one in four Americans. Anthem alone had 80 million records accessed. The hackers who breached Anthem's advanced defenses remained undetected for months.

Crime pays. Accessing health information facilitates identity theft. Identity thieves crave robust medical records with birth dates, addresses, social security numbers, etc. "The value to criminals of having a full set of medical information on a person can go for $40 to $50 on the street. By contrast, a credit card number is often worth just $4 or $5."

Foreign governments (e.g. China, Russia) increasingly initiate attacks. Their expansive programs operate with impunity. They apply Advanced Persistent Threats (APTs) that are patient, careful, nuanced and widespread. They target vulnerable employees, sub-contractors and suppliers.

These are Cyber attacks aren't going away. Current defenses are leaky. Cyber security requires significant tradeoffs between protecting data and maintaining privacy; between data exchange and organizational productivity.

Health companies must appreciate these tradeoffs, increase vigilance and confront the emerging cyber threat head-on. Awareness and employee education are essential. Aware employees can spot atypical data patterns linked to cyber attacks.

Adopting policies of "least privilege" (pro-active data access) and "assumed compromise" (people are suspect until proven otherwise) are cost-effective methods for bolstering cyber defense. Other sensible defensive measures include data encryption, "hack-a-thons" and sharing attack profiles with like-minded companies.

There are two kinds of health companies. Those that have been hacked and those that don't know they've been hacked. Ignorance isn't a defense. Utilizing big data's capabilities comes with the responsibility to protect sensitive information.

The Creepy: Papa Don't Preach

Like many retailers Target collects voluminous data on its customers purchasing patterns. Most shopping is habitual, but big-life events, like getting married, shift buying habits. Retailers use big data analytics to identify customers experiencing a big-life event, so they can lure them into their stores with personalized incentives.

There is no bigger life-event than having a baby. With that in mind, Target developed a model that assigns a "pregnancy prediction" score based on purchases of 25 products during the first 20 weeks of pregnancy. The model also predicts the prospective birth date and enables Target to send sequenced coupons at pre-determined stages of the women's pregnancy (e.g. baby stroller coupons at 7 months). The model worked really well, perhaps too well.

A year after the pregnancy prediction model went live, a father stormed into a Minneapolis Target store demanding to see the manager. His teenage daughter was receiving coupons for baby clothes and cribs. The father wanted to know if Target was encouraging his daughter to become pregnant.

The manager apologized and said he'd look into the matter. He called the man a few days later to apologize again. This time the man was contrite. During an emotional conversation with his daughter, the father had learned his daughter was pregnant. His future grandchild was due that August. Through big data analytics, Target discovered the man's daughter was pregnant before he did.

This story became a public relations disaster for Target. Charles Duhigg reported the Target saga in a cover story, "How Companies Learn Your Secrets," for the New York Times Magazine. Then it went viral in a big way. People freaked out that Target was "spying" on them. Even today, Googling "Target, father, pregnant daughter," generates hundreds of hits. In response to Duhigg's article, Target issued a defensive press release and stopped talking to him.

Here's the thing. Predictive models work. According to Duhigg, Target has earned over a $1 billion predicting which customers are pregnant and marketing products to them. Target and other retailers aren't going to stop using analytics to amplify sales. They are, however, getting much savvier at camouflaging and exploiting their knowledge of individuals' personal information. Buyers be aware.

Big Data's Brave New World

Inevitably, companies and governments will mash healthcare data together with other purchasing, eating, exercise, work and personal financial data to make predictions and judgments about specific individuals. Everyone and everything will have "scores."

Each person's digital footprint will shape their external interactions, often with no discernable indication this is occurring. Big data analytics will influence job hunting, dating, lending and perhaps access to healthcare services.

Like any new technology, big data has potential beneficial and destructive uses. Managing digital reputations and navigating digitized environments are new human experiences. Are we ready?

A version of this commentary appeared in "Academy 360".