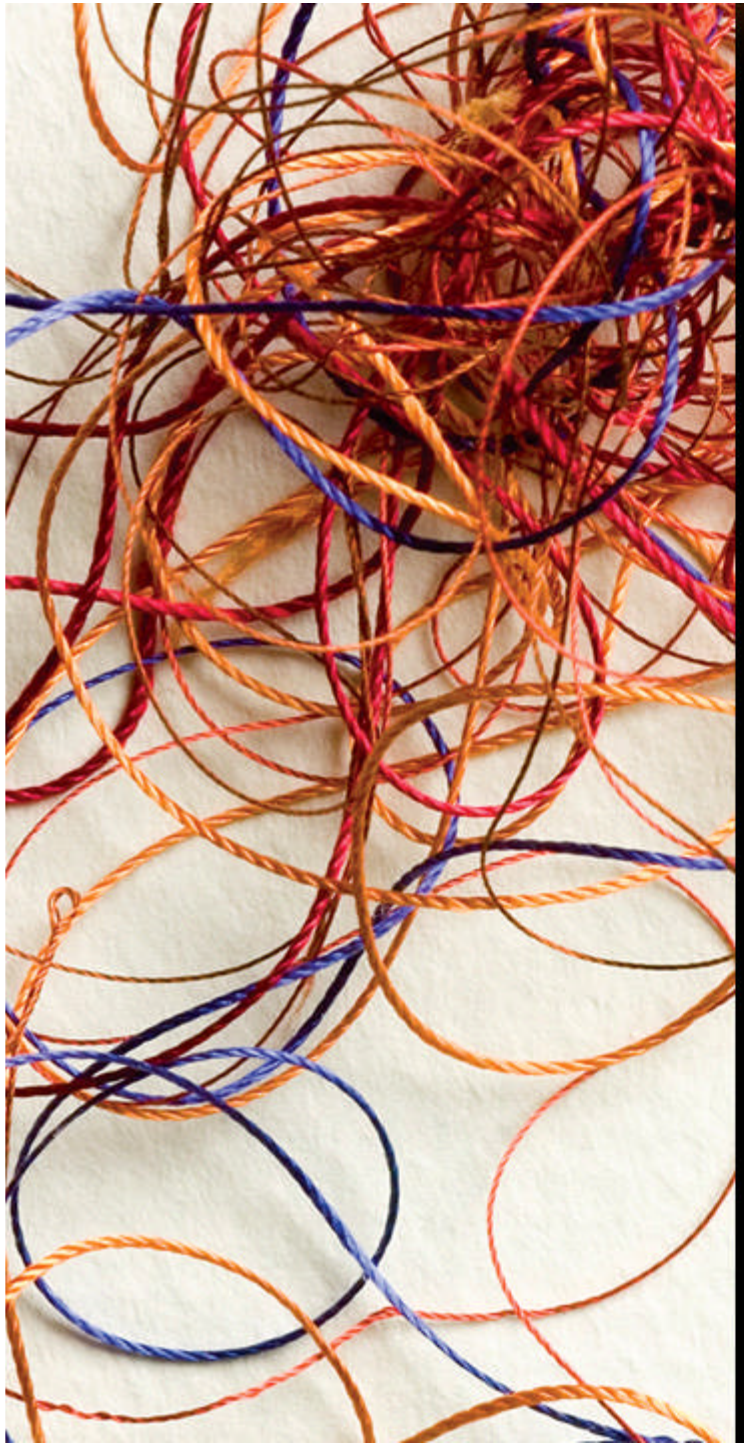


crowell moring

HOOPS 2006

UNTANGLING HEALTHCARE

Information Security Breach Nightmares: How to Protect Your Company Now

Ben Butler & Robin Campbell

October 26-27, 2006

SETTING THE STAGE

- 93,754,333 private records breached in past two years (NYT 9/25/06)
- 81% of companies have faced loss or theft of laptop containing sensitive/confidential info in past year (Ponemon Institute, 8/06)
- Federal contractors experiencing privacy breach in 2004 or 2005 (GAO, 9/06):
  - 47% of Medicare Advantage contractors
  - 42% of Medicare FFS contractors
  - 38% of TRICARE contractors

IMPACT ON FEDERAL HEALTH PROGRAMS

- **Spotlight on Federal agency performance**
  - » V.A. lost laptop – 26.5 million records
  - » Recent GAO Reports
  - » OMB Memoranda

- **Flow down impact on contractors**
  - » Reporting requirements
  - » Auditing & monitoring

MEDICARE ADVANTAGE & PART D

- **CMS 6/9/06 memo: plans must notify CMS of any security breaches involving personal health info**
- **Part D quarterly reports must include number of confidentiality/privacy grievances**
- **OIG "will be assisting CMS in investigating health plan capability in this area."**
  - » Scope of work includes "assessing whether contracted health plans have adequate security controls in place for handling personal health info" (GAO, 9/06)

STATES WITH NOTIFICATION LAWS

- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Kansas
- Louisiana
- Maine
- Minnesota
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Pennsylvania
- Rhode Island
- Tennessee
- Texas
- Utah
- Washington
- Wisconsin

KEY REQUIREMENTS

- **Notification in the event of a breach**
- **Definition of personal information:**
  First name or initial and last name, plus
  - SSN
  - DL number or state ID number
  - Account number, credit or debit number plus security code, access code, or password

VARIATIONS ACROSS STATE STATUTES

- **Broader definition of personal information**
- **Threshold/Standard for notification**
- **Specific time limits**
- **Notification to entities/state agencies in addition to individuals**
- **Content requirements for the notice**
- **Exemptions**
  - » HIPAA
  - » GLB
- **Pre-breach measures**

PRE-BREACH MEASURES

- Similar to HIPAA Security Rule requirements
- Reasonable and adequate security procedures
- Contractual safeguards for transfers
- Effective and timely document destruction methods and policies
- Encryption for transfers

ENFORCEMENT THREATS

- **State Attorneys General**
  - » Injunctive relief
  - » Civil penalties – e.g., Florida, $1000 for each day the breach goes undisclosed for up to 30 days; $50,000 for each 30 day period or portion thereof for up to 180 days, maximum $500,000
  - » Costs and attorneys' fees

ENFORCEMENT THREATS (cont.)

- **Other Civil Litigation**
  - » Private Right of Action – e.g., CA, DE, RI
  - » Class Action litigation – e.g., ChoicePoint, CardSystems, Veteran's Affairs

ENFORCEMENT THREATS (cont.)

- FTC Enforcement Actions
  - DSW
  - BJ Wholesale
  - CardSystems
  - ChoicePoint

FEDERAL BILLS

Numerous—but most prominent are:

- **H.R. 3997**
- **H.R. 4127 [endorsed by Microsoft & Entrust]**

KEY ISSUES/FEDERAL LEGISLATION

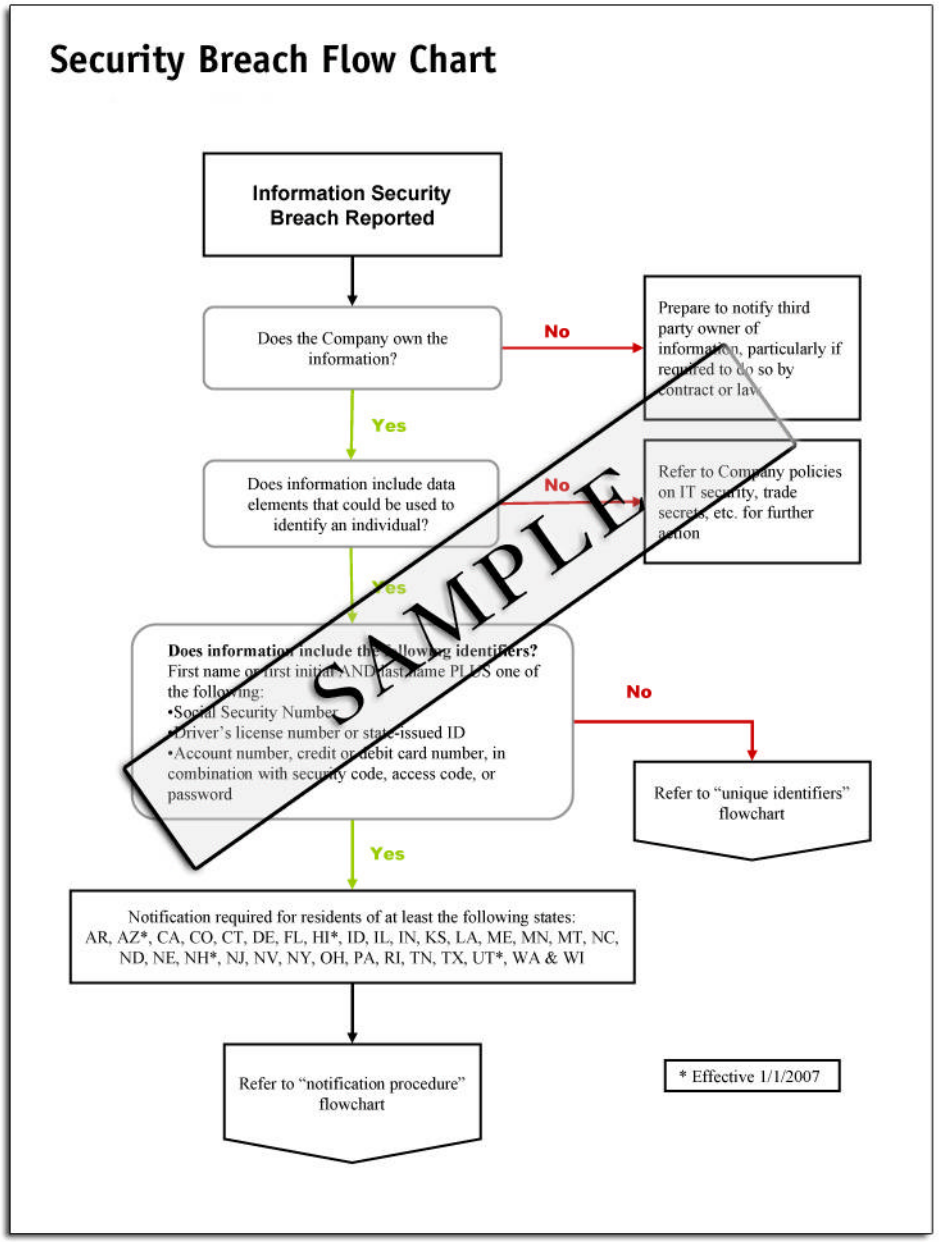
- **Preemption**
- **Breach Reporting Standard/Threshold**
- **Pre-breach Measures**

WHAT YOU CAN DO NOW

- **Inventory personal information**
  - » What do you have and where is it?
- **Assess vulnerability to breach**
- **Benchmark current security against new legal requirements, FTC guidance**
- **Consider alternative use or elimination of personal information**
  - » Change/discontinue use of SSN
  - » Encryption

WHAT YOU CAN DO NOW (cont.)

- **Identify response team – IT, Legal, HR, Public Relations/Communications**
- **Develop template notification form**
- **Prepare templates for injunctive relief if necessary**
  - » Personal information that might constitute trade secret or confidential business information, e.g., HR database or executive compensation information



WHAT YOU CAN DO NOW (cont.)

- **Develop Emergency Response Plan**
  - » Consider flow chart
  - » Assign tasks
  - » Define "breach"
  - » Anticipate contingencies

WHAT YOU CAN DO NOW (cont.)

"HIPAA-esque" measures:

- **Limit access to personal data**
- **Utilize adequate administrative, technical and physical security safeguards**
- **Require adequate security of third parties through contract**
  - » Update existing business associate agreements?
- **Use intrusion-detection technology to rapidly detect breach**
- **Dispose of personal information in an effective and timely manner**

WHAT YOU CAN DO NOW (cont.)

- **Develop contacts at credit monitoring agencies**
  - » Equifax
  - » Experian
  - » TransUnion

- **Train, Train, Train, not just the law, but recognizing suspicious activity and how to protect your organization from a breach**

- **Insurance?**
  - » "AIG Announces Data Breach Product" *Privacy Law Watch* (9/19/06)

CHALLENGES

- **What did we lose / What was accessed?**
- **Who owns the data?**
- **Thoroughness vs. speed**

QUESTIONS?

Ben Butler
(202) 624-2799
bbutler@crowell.com

Robin Campbell
(202) 654-6732
rcampbell@crowell.com