

National HIPAA Audioconferences

Consumer Notification Laws



Davis Wright Tremaine LLP



HIPAA Notification Requirements

- **No automatic notification requirement**
- **Covered entity required to mitigate harmful effects of security incidents – 45 CFR § 164.308(a)(6)(ii)**
- **Unauthorized disclosures to be reported in accounting under Privacy Rule - 45 CFR § 164.538**

State Notification Laws

- **Started with California's SB 1386 – 2003.**
- **Now in about 40 states**
- **Typically require government agencies and businesses to promptly notify individuals whose computerized personal information is reasonably believed to have been obtained by an unauthorized person.**

State Notification Laws

- **“Personal information” typically means an individual’s first name or initial, last name, and SSN, driver’s license number, or State ID card number, or account or bank card number.**
- **In 2008 California added**
 - **Health information**
 - **Insurance information**

State Notification Laws

- **Note that these laws typically apply only to computerized data**
- **It may nonetheless be prudent to notify individuals if a paper record with personal information is stolen**

State Notification Laws

- Typically, individual written notice is required, unless the costs of notice would exceed \$250,000, in which case substitute notice by e-mail, web-posting, and statewide media disclosure may be substituted.

Six Steps to Respond to Data Breaches

1. **Notify internal officials & set up response team**
2. **Determine whether information was “obtained” by an unauthorized person**
3. **Determine who should be notified – individuals, law enforcement, regulators, others?**
4. **Determine what support to offer**
5. **Send notifications**
6. **Respond to inquiries**
7. **Correct security flaws, remediate damages**