

Through the Privacy Looking Glass

Jane Brue,
Compliance Director, LTCG

Glenn Daly, CIPP/US
US Compliance and Chief Privacy Officer,
John Hancock

Stephen A. Serfass
Drinker Biddle & Reath LLP



- Introduction: “New” Era of Privacy?
 - Anthem Update
 - Financial appeal of Medical PHI to Hackers
 - Federal Legislation Proposals
 - New York Insurance Department Activity

- Compliance from the TPA Perspective
- Privacy Risk Mitigation Strategies
- Breach Statistics & Case Studies
- Lessons Learned from Recent Breach Litigation
- Privacy & Genetic Testing

Compliance from the TPA Perspective

- Overview of Data Privacy and Breach Notification Laws
- Emerging Trends
- Effective Privacy Compliance



Privacy and Breach Notification Laws



- **HIPAA/HITECH**
 - Under the jurisdiction of HHS, applies to Covered Entities and their Business Associates with respect to Protected Health Information (PHI)
 - Requires reasonable and appropriate administrative, physical and technical safeguards to prevent improper access, use, alteration, deletion and disclosure of PHI
 - Requires notification in the event of a breach of unsecured PHI
- **GLBA**
 - Under the jurisdiction of the FTC, applies to financial institutions with respect to Nonpublic Personal Information (NPI)
 - Requires companies that offer financial products including LTC insurance to safeguard sensitive data and explain their information-sharing practices
 - LTCI compliance under HIPAA fulfills compliance in many regards
 - Health Breach Notification to the FTC is limited to vendors of personal health records
- **Industry mandates resulting from such laws...**

State Data Security Laws Enacted

as of February 2015



47 jurisdictions have enacted data security laws, which generally:


- Provide definitions of personal information and of a breach of security (most of which limit the definition of breach to electronic or computerized data)
- Specify to whom notification of a breach is required and how soon after discovery
 - All require that the data owner notify individuals*
 - Most require notification to consumer credit reporting agencies*
 - Almost half require notification to other regulatory agencies*
 - 42 have various exceptions*



Big Data Era

- Extraordinary speed of the spread of vast amounts of data
- Blurring of professional / personal lives in social media

Regulations Apply to Breaches Resulting From the Latest Technology

- Vendor as Business Associates vs. unregulated entities
- Risk of harm threshold evolved to a risk analysis of the probability of compromise, and the extent to which the risk been mitigated
- Probability  Possibility

Reaction and Responses to Breaches

- Public response
- Generational perspectives
- Regulatory enforcement



More Breaches are Inevitable...

...as a Result, Anticipate More Enforcement, Regulation and Litigation

Primary Elements of an Effective Compliance Program

Office of Inspector General, U.S. Department of Health and Human Services

1. Written policies & procedures & standards of conduct
2. Governance by a Compliance Officer and committee
3. Compliance training and education
4. Effective lines of communication
5. Application of standards through well publicized guidelines
6. Monitoring and auditing
7. Responding promptly to incidents, with risk analysis and corrective action



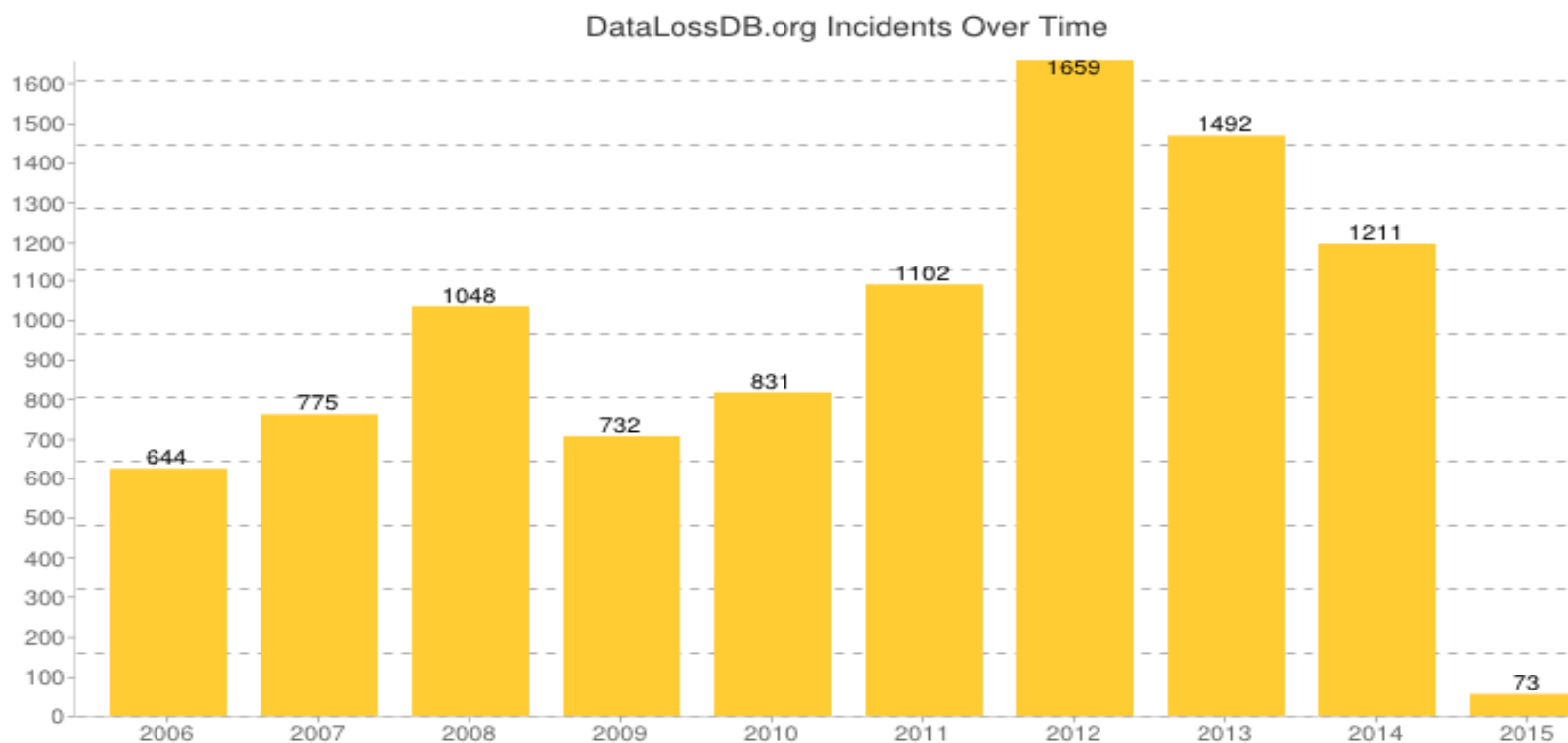
Proactive and Robust Compliance:



- Prevents breaches, regulatory scrutiny and litigation
- Prompts improved quality, increased efficiency, better internal and external public relations
- Is the equivalent of building one's defense in advance, decreasing the likelihood of needing a defense
- Can prevent accusations of negligence or willful neglect, which can draw the heaviest sanctions



Breach Statistics: Number of Reported Data Breaches

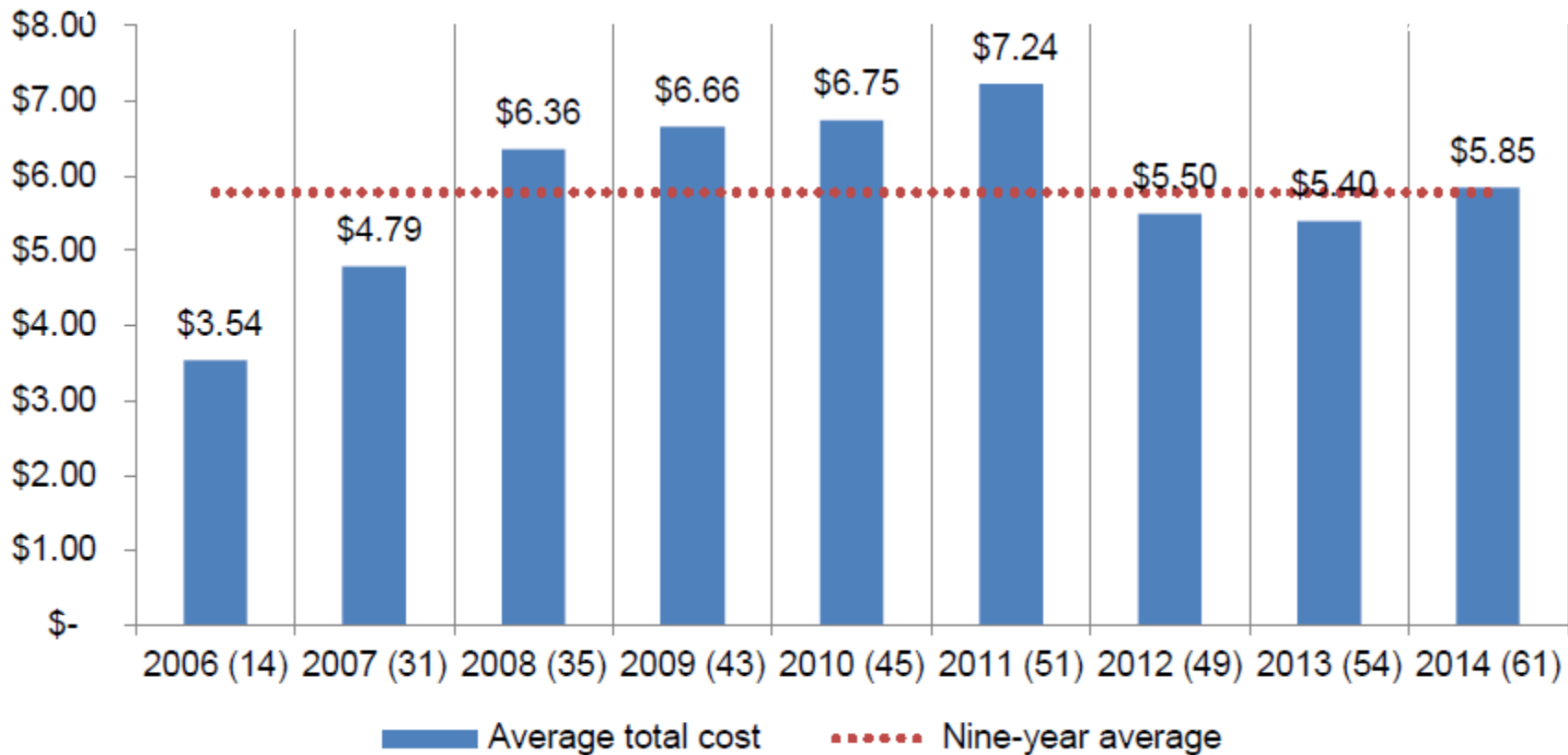


Source: DataLossDB.org

Available at: <http://datalossdb.org/statistics>

Bottom Line: Data breaches are inevitable and, as a result, so is more privacy litigation and legislation

Average Cost of Data Breach (in millions)



Community Health Systems

- August 2014: Tennessee-based CHS reveals that hackers used “highly sophisticated malware and technology” to bypass its servers in April and June of 2014
 - November 2014: CHS reveals attacks originated in China See 8K
- Hackers used computer bug “Heartbleed” to access VPN log-in credentials stored in a test server without security because it was not intended to be connected to the internet
- Accessed non-medical, PHI of 4.5 million people, including SSN, addresses, birthdates and telephone numbers



Community Health Systems Consequences

- Forbes columnist predicts costs could range from \$75-\$150 million
 - Cost Sources: Notification; Remediation; OCR/HHS fines; credit monitoring; defense costs for shareholder, victim class actions, etc.)
- August 21, 2014: First of nine class actions is filed against CHS, only three days after the breach was reported
 - Claims include breach of contract, negligence, violation of the Fair Credit Reporting Act, invasion of privacy, and breach of unfair trade practices
- February 4, 2015: **C**lass actions consolidated in Federal District Court for the Northern District of Alabama



Community Health Systems

- **Lesson:** It does not matter your business line – retail, healthcare provider, insurer – you need to be vigilant about updating security measures and practices
 - Breaches seeking health information will continue to increase because medical PHI can be worth two-three times more than credit card payment information (\$200/\$300 per record vs. \$100 per record)
- Conduct a privacy audit if you have not had one recently to help identify back-door vulnerabilities as in CHS



Affinity Health Plan

- August 2013: HHS settled with Affinity Health Plan, Inc., a not-for-profit issuer of Medicaid managed care plans in NY metropolitan area
- Local CBS affiliate purchased a copy machine previously leased by Affinity; found that machine still stored protected health information of about 344,000 people
- Breach led to an investigation into Affinity's compliance history & current practices



Affinity Health Plan

- HHS and Affinity agreed on a **\$1.2 million fine** and a corrective action plan to ensure future compliance
- **Lesson:** Each type of technology used may present a new area of exposure



The Hospice of North Idaho “HONI”

- An unsecured HONI laptop, containing PHI for 441 HONI patients, was stolen
- January 2013: HHS settled with The Hospice of North Idaho (“HONI”) on a **\$50,000** fine
- First HIPAA breach settlement involving less than 500 patients; no breach too small?



The Hospice of North Idaho “HONI”

- Lesson: encrypt your laptops, as encrypted PHI/NPI may not constitute a breach
 - Increased use of BYOD may lead to more “small-scale” breaches, with “full scale” repercussions
 - Strong policies regulating (or banning) use of personal devices for work and work-issued technology
 - Consider signed consent forms: “I will not use my personal device for work”

“Encryption is an easy method for making lost information unusable, unreadable and undecipherable.”

Former OCR Director Leon Rodriguez



Stanford/Student of Fortune

- 2009: An individual Googled his own name and found it, along with certain health information, in a database that was used on the homework help website, Student of Fortune, to explain how to turn a table into a graph
- Turns out this database was emergency room admissions information from Stanford Hospital misappropriated by a billing vendor

March 2014: Litigation from breach settles for \$4.1M

Difficulties in Pleading Damages, Post-*Clapper*

- *Clapper v. Amnesty International USA*, 133 S.Ct. 1138 (2013)
 - Threatened injury must be “certainly impending” to constitute injury-in fact
 - Plaintiff cannot create standing by taking steps to avoid speculative harm, including incurring costs as a reasonable reaction to a risk of harm
- Post-*Clapper* application to Data Breach Cases:
 - Damages not alleged where allegations limited to (1) potential future harm; (2) monitoring costs for such theft; or (3) non-particularized invasion of privacy (where unauthorized third-party has not viewed information).
 - *See In re Sci. Applications Int'l dCorp. (SAIC) Backup Tape Data Theft Litig.*, 2014 U.S. Dist. LEXIS 64125, at *22-38 (D.D.C. May 9, 2014)
 - *Strautins v. Trustwave Holdings, Inc.*, 2014 U.S. Dist. LEXIS 32118, at *15-22 (N.D. Ill. Mar. 12, 2014)



Breach Litigation: Erosion of Standard

Breach Litigation – No Showing of Damages Required

- *Resnick v. AvMed*, 693 F.3d 1317, 1332 (11th Cir. 2012):
 - Data breach suits are generally dismissed if plaintiffs cannot not show articulated damages
 - The Eleventh Circuit overturned such a ruling and allowed a class action to proceed without articulated damages flowing from the breach for the entire class
 - The case settled in February 2014 with monetary awards available to individuals whose information was stolen but who suffered no articulated damages (\$30 per person not affected)

Breach Litigation: Novel Pleading

- *In re: LinkedIn User Privacy Litigation*, No. 5:12-cv-03088 (N.D. Ca.)
 - Suit under California Unfair Competition Law alleging that LinkedIn's privacy policy misled plaintiff into thinking her data was secure
 - LinkedIn user later suffered a data breach
 - Judge allowed case to proceed past motion to dismiss, reasoning that an allegedly misleading privacy policy is analogous to false advertising



Breach Litigation: Novel Pleading

- *In re: LinkedIn User Privacy Litigation (continued)*
- January 2015: Court tentatively approved \$1.25 million settlement fund; class members can obtain up to \$50 each
 - After \$250,000 in attorneys fees are deducted, would result in about \$1 per affected user if all 800,000 users make a claim
- Formal filing of settlement due by March 24, 2015.

Genetic Testing for LTCi

What Exactly is Genetic Information?



The definition of Genetic Information varies by jurisdiction and by law; genetic information may include the following:

- Information about an individual's genetic tests
- Information about genetic tests of an individual's family members
- Information about the manifestation of a disease or disorder in an individual's family members (*i.e.* family medical history)
- An individual's request for, or receipt of, genetic services

What Exactly is Genetic Information (cont.)?



The definition of Genetic Information varies by jurisdiction and by law; genetic information may include the following:

- Participation in clinical research including genetic services (by the individual or a family member of the individual)
- Genetic information of a fetus carried by an individual or by a pregnant woman who is a family member of the individual
- Genetic information of any embryo legally held by the individual or family member using an assisted reproductive technology

- Federal Law
 - Statute: GINA (Genetic Information Non-Discrimination Act)
 - Regulations promulgated by:
 - Department of Health and Human Services
 - Department of Labor
 - Department of Treasury
- State Law
 - State statutes and regulations vary and can be stricter than federal law

- Statute initially passed in 2008
- Includes a Prohibition on use of genetic information for underwriting purposes for:
 - Group health plans
 - Health insurance issuers (including HMOs)
 - Issuers of Medicare supplemental policies

- (Applies to Health, but does not presently apply to LTC)
- Prohibits the use and disclosure of genetic information for underwriting. May not use genetic information for:
 - eligibility determinations,
 - premium computations,
 - applications of any pre-existing condition exclusions
 - life, disability, LTC exempted

Source: Pub. L. 110-233, 122 Stat. 881, enacted May 21, 2008

- Mega Rule leaves the door open to future extension to LTC
 - Specifically says HHS has authority to expand prohibition on use of genetic information beyond defined “health plans”
 - “[I]ndividuals have a strong privacy interest in not having their genetic information used in an adverse manner for underwriting purposes...”
 - But, HHS recognized that extending prohibition to LTC carriers may affect viability of LTC insurance market

State Law Impact on Use of Genetic Information

- Federal law provides a *floor*, not a *ceiling*
- 50 states = possibility for 50 state laws
- 4 General Categories of State Law on the Use of Genetic Information in Underwriting
 - No guidance
 - Liberal: Permitted
 - Moderate: Permitted, with restrictions
 - Restrictive: Prohibited

Genetic Testing: Maine (Liberal)



- Insurer **may use** genetic test results in issuing, withholding, extension or renewal of policy
- Insurer **may require** genetic testing
 - Insurer must comply with certain requirement, such as obtaining authorization
- In using genetic information, insurer **may not unfairly discriminate** based on genetic information or the results of a genetic test
 - Unfair discrimination: applying test results or genetic information in a manner not reasonably related to anticipated claims experience
 - Genetic information: information concerning genes, gene products or inherited characteristics that may be obtained from an individual or family member

Source: 24-A M.R.S.A. § 2159-C

Genetic Testing: Massachusetts (Moderate)



- Insurer **may not require** a genetic test to issue or renew policy
- Insurer **may ask** on application whether the applicant has taken genetic test
 - Applicant not required to answer the question.
- Insurer **may use** genetic information submitted by applicant
- Insurer **may not unfairly discriminate** based on the results of a genetic test or the provisions of genetic information
 - Unfair discrimination: Using information that is unreliable or not reasonably related to insured's mortality or morbidity, based on sound actuarial principles, or actual or reasonably anticipated experience

Source: Massachusetts General Laws Annotated, 175 § 108I

Genetic Testing: Maryland (Restrictive)



- Insurer **may not request or require** genetic test, the results of a genetic test, or genetic information to deny coverage or raise premium
- Insurer **may not use** a genetic test, the results of a genetic test, genetic information, or a request for genetic services to deny coverage or raise premium
 - Genetic information: includes information “about chromosomes, genes, gene products, or inherited characteristics that may derive from an individual or a family member”

Source: MD Code, Insurance, § 18-120

- Predictive Modeling – Slippery Slope?
 - Devises statistical tools to identify systematic patterns in genetic information, and turns this information into business rules, with the goal of achieving better decision making
 - Standard underwriting techniques are costly and time consuming; underwriting process can be made faster, more economical, more efficient, and more consistent
- Consumer Backlash?



- Increased use and storage of data
 - 2000: 5 million terabytes of data
 - 2011: 2 billion terabytes
 - 2015: projected to be 8.5 billion terabytes
- Variety of data stored
 - GPS, videos, music, photos, consumer purchases, app downloads, search queries, tweets, wiki publications
- The Role of Analytics
 - Ability to identify individuals through the variety of data collected
- Happening at a very fast rate
 - More than 250 billion photos have been uploaded to Facebook; more than 350 million photos are uploaded each day on average
 - Amounts to approximately 10 photos per month per Facebook user

Framing the Debate

- Use of genetics in insurance?
 - Pricing policies differently based on individuals' genetics
 - LTCi – different pricing based on Female v. Male
- Corporate entities using insured's private genetic information against them for pricing products
 - Unethical or good business?

- Is it ethical for an insurer to use genetic information to make an adverse decision against an individual with certain genetic markers?
- If a State has no law or liberal laws regulating the use of genetic information, is it ethical to use such information?

QUESTIONS?
(we will be available
after the presentation as well)

Thanks for attending!

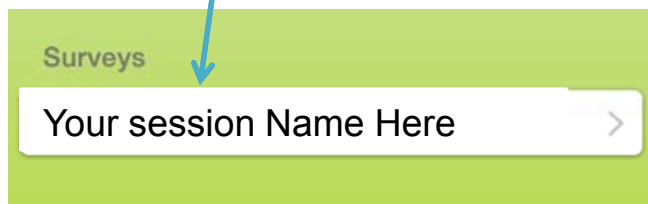
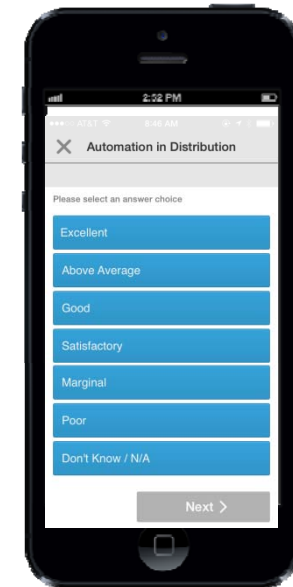
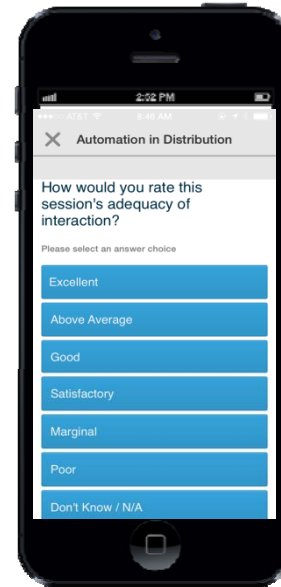
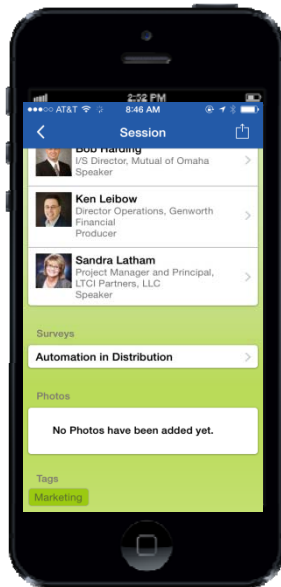
Don't forget to fill out the survey



1st you must have download the ILTCI Mobile App
- Go to your app store; search ILTCI. It's free.



1. Find the session
2. Scroll to the bottom
3. Tap on the session name below the survey



Tap on the answer you wish to submit

Click Next