# Helping Employers and Their Benefit Plans Address and Mitigate Data-Related Risks

Brian Bartels, Partner

June 2019

KUTAKROCK
kutakrock.com

## Agenda

- Data privacy, security, and confidentiality issues for employee benefit plans
- Data privacy, security, and confidentiality issues for employers
  - Internal policies and procedures
  - Employment laws that affect data privacy/security/confidentiality
- Obtaining management buy-in and training employers and employees
- Questions

# Employ Benefit-Related Issues



KUTAKROCK

## What are Employee Benefits?

- Medical, dental, vision, and prescription drug coverage
- Short-term and long-term disability, accidental death and dismemberment, business travel accident, and life insurance
- Cafeteria plan, dependent care assistance program, and health flexible spending arrangement
- Wellness programs
- Employee assistance programs ("EAPs")
- 401(k) and defined benefit pension plans
- Deferred compensation arrangements
- Executive compensation

 Questions? Email Polls@KutakRock.com

KUTAKROCK

# Employee Benefit Plans are Data Driven

- Eligibility, enrollment, and beneficiary designations typically require data for the employee, a spouse, and any dependents
  - Name
  - Date of birth
  - Social Security number
  - Address
  - Telephone number
  - Compensation information
- Data typically shared with various parties, such as human resources, payroll provider, insurance companies, and third-party administrators



# Key Considerations for Protecting Data

- Health plans
  - HIPAA policies and procedures
    - Training
    - Breaches
  - Business associate agreements
    - Insurance
    - Indemnification
  - Administrative services agreements
    - Insurance
    - Indemnification
    - Where data resides
    - Subcontractors

# Key Considerations for Protecting Data

- Wellness programs
  - ADA
  - GINA
  - HIPAA
- Retirement plans
  - Not HIPAA
  - Disability portions of plan may have ADA or GINA issues
  - Privacy around SSNs, financial data

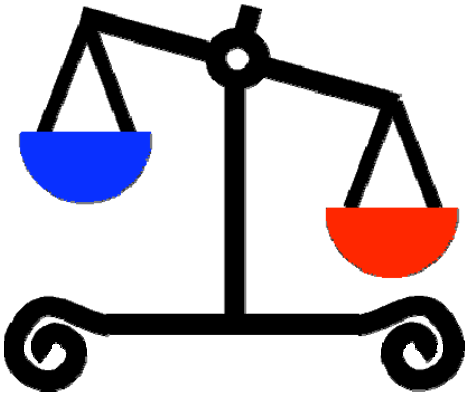


# Privacy/Security and ERISA Fiduciary Duties

- Duty of care
- Duty of loyalty
- Duty to follow plan documents
- Duty to prudently invest plan assets
- What if breach is caused by a plan fiduciary?

# Cyber Liability Insurance

- To Have or Not to Have





# Cyber Liability Insurance | Coverage Gaps

| Errors & Omission | General Liability | Property Insurance | Crime Insurance |
|---|---|---|---|
| • Typically excludes a security breach<br>• Typically tied to / requires an act of negligence to trigger coverage | • Excludes damage to and corruption of electronic data<br>• Covers only "tangible" property<br>• Excludes damage or injury resulting from intentional acts<br>• Personal & advertising liability does not cover violations/misuse of private information | • Coverage is specific to physical loss or damage to tangible property (named)<br>• Courts have consistently held that data is not tangible property | • Covers loss due to employee theft of money, securities or other property<br>• Property must be tangible and have intrinsic value<br>• No coverage for confidential information |

# Not All Cyber Liability Insurance is Equal

- Policies are often written as excess and surplus coverage, as a result not regulated by the states.
- Lack of uniformity – each carrier has its own coverages and exclusions.
- Negotiation of coverage.
  - Some policies only respond if the insured is legally required to respond to a security incident – may be in the best interest of the insured to respond regardless of a legal requirement.
  - Credit monitoring services.
- Some policies exclude breaches of third-party vendor data systems.
  - Limitations on coverage for data not on the insured's system. (i.e., cloud providers and IT hosting).
  - Make sure contract provisions and insurance coverage address gaps.



# Examples of Cyber Liability Insurance Issues

- First party liability coverage.
- Third party liability coverage.
- Coverage sub-limits.
- Retroactive coverage date.
- First party contingent/dependent business interruption. (This coverage is important if data is housed on a third-party's system.)
- Exclusions for breach of contract.
- Coordinated retention endorsement (only one deductible/breach event).
- Choice of counsel.

# Employer Policies

## *Addressing Data Security*



KUTAKROCK

## Personnel Files

- Used to collect and store information about employees – often sensitive, personal, embarrassing
- E.g.:
  - Background check
  - Disabilities, medical conditions, accommodations, need for leave
  - Biometric data
  - Home/personal address and contact information
  - Legal proceedings
  - Social security and other identifying information

 Questions? Email Polls@KutakRock.com

KUTAKROCK

## Personnel Files

- Best practice: internal procedure to ensure appropriate retention and storage of employees' personal information
- Elements include:
  - Separate information into appropriate (confidential) files
  - Avoid "desk" files
  - Assign responsibility for maintenance
  - Limit access
  - Destruction schedule



## Biometric Data

- Personal data relating to physical, physiological, or behavioral characteristics which allow or confirm the unique identification of that person
- Examples:
  - Fingerprints
  - Eye scans
  - Facial recognition
  - Ear canal authentication

## Biometric Data

- Washington, Illinois, and Texas already have laws regulating this area (others likely to follow suit) – with penalties
  - Some courts have held breach of statute (without actual injury) enough to convey standing for claim
- Tort claims
  - Invasion of privacy
  - Intentional infliction of emotional distress



## Biometric Data

- Obtain consent in writing prior to collection of biometric data
- Negotiate with unions (if applicable) prior to collection
- Written policy
  - Reason for collection
  - Explanation of technology
  - Manner in which data will be stored – including safeguards
  - Destruction procedure

# Monitoring Employee Communication and Use of Company Systems

- Courts typically permit employers to monitor:
  - Communications made in course of employment
  - Use of company systems (telephone, email, internet, VPN)
- But -> increases duty of care regarding information employer now expected to know
- Increases likelihood of claims by employees
  - Invasion of privacy
  - Violation of SCA
  - Publication of private facts



# Monitoring Employee Communication and Use of Company Systems

- Best practice: written policy expressly stating that employer reserves the right to monitor communications or use of systems, and employees have no right to privacy in:
  - Work communications/use of systems made on private devices
  - Private communications made on company devices or using company systems
- Policy should also provide that there is to be no texting for work purposes/tasks

## Monitoring Employee Communication and Use of Company Systems

- Social media
  - New platforms
  - Cannot force employees to provide passwords or access
  - Avoid connecting with employees on social media
  - Avoid reviewing data publicly available on social media
- Occasionally employers may have a duty to review social media
- Policy should limit use during working hours and via company systems or equipment



## Bring Your Own Device (BYOD)

- Pros
  - Less expensive
  - Employees prefer choice
- Cons
  - Reduces employers' ability and right to access device or information on device (increases employees' right to privacy)
  - Greater IT costs related to maintenance
  - **Reduced security**

## Bring Your Own Device (BYOD)

- BYOD Policy
  - Limits acceptable devices
  - Limits employees permitted to BYOD
  - Requires consent in writing to access/monitoring (limiting claim of loss of privacy in personal information)
  - Requires passwords, encryption software, updates, frequent backups



## Bring Your Own Device (BYOD)

- BYOD Policy
  - Requires employees to be trained on security practices
  - Requires employees to physically protect device and notify employer of its loss
  - Employers should put a remote-wipe feature in place to purge data before lost or broken device is replaced
  - For departing employees, employers should collect, review and image devices, and then wipe

## Confidentiality Policy

- Policy protects disclosure of all company confidential information, including information, data or documents related to employees
- Definition of confidential information should be encompassing but specific
- If the policy precludes discussion of wages or working conditions, it could result in NLRB penalties – consider two or more policies
- Policy can be exchanged for or supplemented by non-disclosure agreement



## Employment Law

*Laws affecting privacy, security, and confidentiality*

# Legal Duty to Protect Confidential Employee Medical Information

- Employers may come into contact with employee or job applicant health information in a number of ways, such as:
  - Post-offer medical examination;
  - Work-related injury;
  - Requests for medical leave; or
  - Requests for disability accommodation.



# Americans with Disabilities Act (ADA)

- The ADA requires employers that obtain disability-related medical information to maintain it in a confidential medical file that is kept *separate* from the employee's personnel file.
  - Obligation applies to prospective hires and current and former employees.
- Such information may be disclosed *only* in limited situations and to individuals specifically outlined in the regulations:
  - Supervisors and managers who need to know about necessary work restrictions or accommodations;
  - First aid and safety personnel, if a disability might require emergency treatment; and
  - Government officials investigating compliance with the ADA.

# Examples of ADA Protected Information

1. Results of a medical exam done at the request of an employer at any time.
2. Medical information shared during the hiring process.
3. Information about a disability submitted on an affirmative action form.
4. Medical information given to request an ADA accommodation.
5. Medical information given in an employer's health and wellness program.
6. Medical information accidentally obtained by an employer.



OG1

# Genetic Information Nondiscrimination Act (GINA)

- Employers generally should not request or require information about an employee or job applicant regarding that individual's genetic information (e.g., information about an individual genetic tests, genetic tests of a family member, or family medical history).
- Employers that acquire such genetic information must treat it as a confidential medical record in a *separate* medical file.
  - Same file as disability-related information?
  - Different rules apply regarding when and to whom genetic information may be disclosed.

## Slide 86

**OG1** O'Hara, Gillian, 2/16/2019

# Treatment of Paper and Electronic Records

- ADA and GINA require confidential treatment of medical information.
  - Paper records must be kept in separate medical files and treated as a confidential.
  - Equal Employment Opportunity Commission (EEOC) expects locked storage cabinets or locked rooms where paper records are kept.
- The EEOC does not interpret either statutes' confidentiality provisions as applying only to paper records.
  - Neither the ADA nor GINA specifically addresses the need for electronic security.
  - The EEOC specifically mentions encryption, password authorization, and "other security safeguards" for electronic records maintained by employers.



# Family Medical Leave Act (FMLA)

- The FMLA authorizes two types of claims – interference and retaliation.
- Under the FMLA, records and documents relating to:
  - **Certifications, recertifications or medical histories** of employees or employees' family members, created for purposes of FMLA, shall be maintained as confidential medical records in separate files/records from the usual personnel files.
- It is unsettled whether this provision gives rise to a private right of action for disclosure and courts have ruled both ways on the matter.
  - Courts that allowed claims to survive have construed disclosure of an employee's confidential medical information to constitute both interference with FLMA rights, and retaliation where disclosure materially affected working conditions.

# Other Laws Related to Confidential Medical Information

- State law:
  - State law counterparts may have more expansive scope.
  - Additional state laws may apply.
- State civil rights law: Generally require confidential treatment of medical information in separate file except under certain circumstances.
- Drug testing records: Most state drug testing statutes require nondisclosure and confidential treatment for results, with certain exceptions.
- Section 504 of the Rehabilitation Act: Applies to federal agencies receiving federal monetary assistance and incorporates by reference the confidentiality obligations of the ADA.
- Occupational Safety and Health Act (OSHA): Occupational exposure records under OSHA may also qualify as medical information under the ADA.



# Other Laws Related to Confidential Medical Information

- Workers' compensation: Each state workers' compensation act is different and disclosure of medical information varies from state to state.
  - If medical information comes into the possession of the employer through a worker's compensation claim, it should be treated in accordance with other federal and state laws covering the treatment of confidential medical information.
- Fair Credit Reporting Act (FCRA): When job applicant is asked to submit to a background check, the FCRA restricts consumer reporting agencies from including medical information in background checks unless job-related and employee has provided written consent.

# Management

## *Buy-in and Training*



KUTAKROCK

## The Starting Point

- A primary reason organizations are concerned about privacy and data security is because of the associated RISKS
- Organizations are typically motivated by various considerations, such as:
  - Maintaining regulatory compliance
  - Avoiding liability
  - Preserving reputational goodwill
  - Ensuring that critical business functions are not disrupted (avoiding "downtime")

 Questions? Email Polls@KutakRock.com

KUTAKROCK

## Why Is the C-Suite Important?

- Without the support of senior management, the following essential elements of an organizational privacy and data security risk management program are likely to fail:
  - Fostering an organizational culture in which privacy and data security are valued and promoted
  - Providing adequate financial and human resources to build out and maintain a robust information security management program
  - Enforcing programmatic policies and procedures
- Without the full support of the C-Suite, in these three key areas, effective risk management simply cannot occur



## How to Engage the C-Suite

- 6 proven strategies for C-Suite engagement:
  - Create an executive-level Information Security Risk Management Committee (ISRMC)
  - Require C-Suite participation in security awareness training
  - Track and report security incidents to the C-Suite and/or ISRMC on a regular basis
  - Run information security tests, and share the results with the C-Suite and/or ISRMC
  - **Bring in the insurance brokers and underwriters to talk about information security risk mitigation**
  - **Quantify the risk in monetary and regulatory (penalty) terms**

## Security Awareness Training

- New hire, annual, and refresher training is crucial to:
  - Communicate and explain company policies, both (1) those that affect employees, and (2) those that require employee implementation
  - Reinforce that privacy and data security are an important part of the organizational culture
- While C-Suite participation in training should be a given, it is not uncommon for members of the C-Suite to exempt themselves from organization-wide training requirements



## Security Awareness Training

- Privacy and information security training is one area where 100% participation should be mandatory, since organization-wide security is only as good as your weakest link – and there have been instances where that weak link is the CEO.
- Incorporating into training plenty of real-world examples of information security catastrophes is a great way to heighten senior management's awareness of the risks!

## Bring In the Insurance Broker and Underwriters

- In educating the C-Suite, your cyber-insurance broker and underwriters are your allies!
- The insurers can talk to the C-Suite authoritatively about both risks and successful mitigation strategies.
- As importantly, they can help quantify the risk in monetary terms – and may be able to correlate the cost of mitigation strategies with potential reductions in insurance premiums.



## Quantify the Risk

- Regarding regulatory risk, some laws that are easy attention grabbers include:
  - HIPAA, which imposes both civil and criminal liability in certain instances
  - California's new Consumer Privacy Act, which will impose penalties of $2,500-$7,500 per violation and statutory damages of $100-$750 per record or incident, in the event of a breach
  - Corporate liability for individual employee's privacy violations under the legal theory of "respondeat superior" (the *Walgreen's* case)

# Questions?



# *Thank You*

This presentation was developed by contributions from the following attorneys in our Employee Benefits, Employment Law, and Data Privacy/Security practices.

**P. Brian Bartels**
**Employee Benefits**
Omaha

**Cindy L. Davis**
**Employee Benefits**
Minneapolis

**Ruth S. Marcott**
**Employee Benefits**
Minneapolis

**Kasey M. Cappellano**
**Employment**
Omaha

**Gigi O'Hara**
**Employment**
Omaha

**L. Elise Dieterich**
**Data Privacy/Security**
Washington, D.C.