HELPING EMPLOYERS MANAGE PRIVACY IN THE WORKPLACE

Laws, Communications, Monitoring, Risk Management and More

Charles M. Russman
(248) 988-5868
crussman@clarkhill.com

CLARK HILL

THE DATA YOU HAVE

- Name and contact information
- Health Information
- Sexual preference
- Financial Information
- Union membership
- Social Security Number
- Family information

PERMISSIBLE USE AND PRUDENT USE

- Just because you can, does not mean you should and does not control how you should

SPECIFIC LAWS

- Social Security Numbers

SPECIFIC LAWS

- Expectations of privacy exist, especially for non-employee participants in employee benefit plans

HIPAA

- Use PHI only as permitted by HIPAA
- Use the minimum necessary
- Obtain appropriate agreements
- Conduct a risk assessment
- Implement appropriate administrative, technical and physical safeguards
- Train your employees

HIPAA TIPS

- When possible, consider not receiving health information
- Workers compensation
- FMLA

FINANCIAL ACCOUNT INFORMATION

- Even if no law, such as HIPAA applies, most state laws will apply

FINANCIAL ACCOUNT INFORMATION

- This is data particularly prone to identity theft and HR can be a weak point for obtaining it if employers are not careful

FINANCIAL ACCOUNT INFORMATION

- Transfers and vendors are particular weak points for cybersecurity

EMPLOYEE TRACKING

- Monitoring employees comes with many risks, legal and otherwise

EMPLOYEE TRACKING

- What about apps that track employee productivity and location?

FTC ACT

- Benefits, payroll and other portals can be subject to the FTC Act
- So can portals with vendors

CALIFORNIA AND EUROPE

- These are broad laws with broad reach

CALIFORNIA AND EUROPE

- Employees need to be informed about:
  - How you collect data
  - How you use data
  - How you disclose data and
  - Who to contact with questions or to exercise their rights

CALIFORNIA AND EUROPE

- Informing employees is not enough
- You also need to train employees, get agreements in place and have practical policies for compliance

CALIFORNIA AND EUROPE

- Make sure data is kept confidential, available and resilient
- Cannot treat people differently if they exercise their rights

CALIFORNIA AND EUROPE

- Consent should be a last resort and must be done right
- Have someone designate to have responsibility for compliance and as a contact person

CALIFORNIA AND EUROPE

- Watch for employee expectations
- Customer and vendor obligations

CONSENT REQUIREMENT

- Proactive
- Informed
- Understandable
- Recorded
- Affirmative
- Voluntary

EMPLOYEES AND SOCIAL MEDIA

- Employee use about work is different from their other use personal use

EMPLOYEES AND SOCIAL MEDIA

- It can be risky business to view, access or act on an employee's social media profiles or postings

VENDORS

- Most privacy laws require you to obligate vendors to comply with applicable law and your written policies
- Failure to document is often a violation

VENDORS

- Do not assume standard privacy or confidentiality language will suffice
- Neither will standard limitations on liability or indemnification

RISK ASSESSMENT

- Required by several privacy laws, they are an effective and practical way to determine your risk, the potential costs and where (and how) to focus on ensuring compliance

RISK ASSESSMENT

- Objectively assess the risk
- Use clear standards
- Involving the right people
- Ask the right questions

DATA BREACH LAWS

- State cybersecurity laws apply when you have data from an individual who resides in the state or you reside in that state

BREACH ASSESSMENT

- Know the requirements and who is responsible for making decisions

DATA BREACH PLANNING

- Have a plan for each major risk you face
- Planning could reduce or eliminate notice requirements
- Employee training and expectation setting are essential

DATA BREACH PLANNING

- Open and honest communication can make a big difference
- Know who you will contact and what you will say when you do contact people

DATA BREACH LAWS

- What data does the law apply to?
- What about encryption?
- How and when do you notify individuals?
- Do we need to notify the government?
- What details should be included?
- Do we provide credit monitoring?

QUESTIONS?

Charles M. Russman

(248) 988-5868

crussman@clarkhill.com

THANK YOU

Legal Disclaimer: This document is not intended to give legal advice. It is comprised of general information. Employers facing specific issues should seek the assistance of an attorney.

CLARK HILL