



Genetics and Cybersecurity: Not Science Fiction Anymore

Presented by:
Julie C. Theall and Frankie T. Jones, Jr.
Smith Moore Leatherwood LLP
525 North Tryon Street
Charlotte, NC 28202
T: 704-384-2656
F: 336-433-7478

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

The Genetic Information Nondiscrimination Act (“GINA”)

- Employers of 15 or more
- Prohibits employers from requesting, requiring or purchasing genetic information
- Enforced by EEOC
- EEOC issued regulations in November 2010



The Genetic Information Nondiscrimination Act (“GINA”)

- EEOC Activity
 - More than 200 charges since late November 2010
 - On rise
 - Typically included with ADA (disability) charge
 - “newly minted” investigators and increased funding



Genetic Tests

“Analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes.”

- Test for genetic variant for:
 - Huntington’s
 - Breast Cancer
 - Sickle Cell Anemia
 - Spinal Muscular Atrophy
 - Fragile X Syndrome



Not Genetic Tests

- Tests for
 - HIV/AIDS
 - Pregnancy
 - Alcohol / Drug
 - Cholesterol



Not Genetic Information

- Medical information on *Current* Illness
- E.g., employee’s ability to work limited by Huntington’s
- Consider ADA reasonable accommodation
- Consider FMLA leave (intermittent)




Employment Physicals

FAMILY HISTORY: Have your parents, brothers, or sisters ever had any of the following diseases? Please indicate by an (X) in the box.

Tuberculosis	()	Kidney Disease	()	Diabetes	()
Cancer	()	Heart Disease	()	Epilepsy	()
Liver Disease	()	Mental Disease	()	High Blood Pressure	()

I understand and agree that misrepresentation or omission of fact on this physical examination form may cause for cancellation of the application or separation from service of the company.


Signed: _____ Date: _____



The Genetic Information Nondiscrimination Act ("GINA")


Focus on the present, not the future.

Family history has nothing to do with whether an employee can do the job RIGHT NOW.



Genetic Information

- Remove requests for family health history or other genetic information from all employment-related requests for Medical Information
 - Pre-employment physical
 - Request for medical leave for employee
 - Request for health information to support ADA accommodation, use of sick days



Inadvertent Disclosure Exception

- The “Water Cooler” Exception
- Don’t Ask – Don’t Tell
- Listen, Don’t Probe



SMITHMOORE
LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP. All rights reserved.

Safe Harbor

The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA Title II from requesting or requiring genetic information of an individual or family member of the individual, except as specifically allowed by this law. To comply with this law, we are asking that you not provide any genetic information when responding to this request for medical information. “Genetic information,” as defined by GINA, includes an individual’s family medical history, the results of an individual’s or family member’s genetic tests, the fact that an individual or an individual’s family member sought or received genetic services, and genetic information of a fetus carried by an individual or an individual’s family member or an embryo lawfully held by an individual or family member receiving assistive reproductive services.

SMITHMOORE
LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP. All rights reserved.

Inadvertent Disclosure

Without the warning, if family health history is disclosed, EEOC will likely find liability.



SMITHMOORE
LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP. All rights reserved.

Inadvertent Disclosure

- Questions about employee's general well-being:
 - How are you today?
 - Did they catch it early?
- Volunteered information
 - My mother was just diagnosed with cancer



Inadvertent Disclosure

- May ask for a “doctor’s note” to explain an absence
- Even without warning, EEOC does not consider this request to be “made in a way likely to result” in disclosure of genetic information



Inadvertent Disclosure

Be careful what you ask. . . It might just hurt you.

- Discrimination = State of Mind
- And, once known.....



Exception - FMLA

- Except: FMLA medical certification for family member
- Use the Department of Labor form: WH-380-F



Wellness Programs

- May involve use of genetic information
- Must have prior, voluntary, knowing and written authorization
- Genetic information may be provided by employee to healthcare provider (and vice-versa)
- Only aggregated information may be provided to the employer



Retaliation

Be Careful:

- Watch Wellness Program incentives
- May request genetic information
- But must be voluntary participation
- Genetic medical monitoring is ok (if required by law or voluntary)



Health Benefits

- Cannot use genetic information to make decisions as to whether individual can participate
- Health benefits are a term or condition of employment
- Cannot refuse to hire or terminate due to anticipated health costs
- Title I limits use of genetic information in setting premiums and providing coverage



GINA = Confidentiality

- Safeguard Genetic Information
- It is *illegal* to disclose genetic information to third parties
 - Segregate it
 - Require a specifically worded court order
 - A subpoena for "personnel file" or "all employment files" is insufficient



Remedies

- Same as Title VII
- Hiring, reinstatement, promotion
- Back pay, compensatory/punitive damages
- Damage caps 50 (under 100)
300k (over 500)
plus attorney's fees



The North Carolina Identity Theft Protection Act



Primary Components of ITPA

- Document disposal
- Use and disclosure of social security numbers
- Notification requirements in the event of a security breach



Entities Covered by the ITPA

- All businesses that do business in NC or do business with NC residents
- Governmental entities



Exemptions

- Financial Institutions
- Consumer Reporting Agencies
- Health Insurers
- Health Care Facilities

BUT: only exempt from rules on document disposal



What if I Violate the ITPA?

- Financial penalties, including
 - Treble damages
 - Attorney fees
 - Civil fines if brought by Attorney General's office



Document Disposal
N.C. General Stat. §75-64
(December 1, 2005)



Document Disposal Policy

- Requires adopting written policies for disposal of personal identifying information
 - Electronic records
 - Paper records
- Monitor compliance



SMITH MOORE
LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP. All rights reserved.

What Personal Identifying Information is Covered by the Disposal Policy?

- Social security number
- Taxpayer ID number
- Drivers license number
- Passport number
- Bank account numbers
- Credit/Debit card numbers
- PIN numbers



SMITH MOORE
LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP. All rights reserved.

What Personal Identifying Information is Covered by the Disposal Policy?

- Email names or addresses
- Internet account numbers/ID names
- Digital signatures
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage



SMITH MOORE
LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP. All rights reserved.

Approved Disposal Methods

- Burning
- Pulverizing
- Shredding
- Special considerations for electronic data



Disposal By Third Party Vendors

- Due Diligence—Action Is Required!!
 - Review audit
 - Obtain references
 - Check certification
 - Evaluate their disposal policies and procedures



PROTECTION OF SOCIAL SECURITY NUMBERS

N.C. Gen Stat. § 75-62
(October 1, 2006)



Protection for Social Security Numbers

–ITPA limits:

- Collection
- Use
- Disclosure



ITPA Specifically Prohibits

- Disclosing SSN to the general public
- Printing or imbedding SSN on cards that access products or services
- Requiring transmittal of SSN over the Internet unless encrypted

ITPA Specifically Restricts

- Requiring a social security number to access an Internet website
- Printing SSN on mailed materials
- Selling, leasing, loaning, trading, renting or disclosing SSN to a third party without written consent

Permissible Use/Disclosure of Social Security Numbers

No written consent needed to use SSN for:

- Contracts, account and policy applications
- Credit reports
- Background checks
- Last 4 digits



Step 1

• Adopt a Written Policy

- Define "personal identifying information"
- Commit to keep PII confidential
- Commit to collect only necessary PII
- Commit to reduce use of SSNs
- Commit to secure all PII



Step 1

• Adopt a Written Policy

- Commit to dispose of PII properly
- Commit to respond to security breach
- Commit to train employees
- Commit to monitor compliance, regular audit
- Commit to discipline offenders



Step 2

Appoint a Privacy Committee and Officer



SMITH MOORE
LEATHERWOOD
© 2014 Smith Moore Leatherwood LLP. All rights reserved.

Step 3

- Analyze Current Practices

- Each department/function must analyze and report:

- (1) What PII is collected?

- Form review
- Assess timing and manner of collection
- Analyze flow of information
- Assess necessity

SMITH MOORE
LEATHERWOOD
© 2014 Smith Moore Leatherwood LLP. All rights reserved.

Step 3

- Analyze Current Practices

- Each department/function must analyze and report:

- (2) Is the PII collected secure?

- Is access limited? Can we track users?
- Physical protection (location, locks)
- IT protection (firewalls, password)
- Background checks on custodians

SMITH MOORE
LEATHERWOOD
© 2014 Smith Moore Leatherwood LLP. All rights reserved.

Step 3

- Analyze Current Practices
 - Each department/function must analyze and report:
 - (3) When and how do we dispose of PII?
 - Do we have a document retention plan?
 - Are we using disposal methods that ensure confidentiality?
 - Physical documents and electronic data



Step 4

- Develop procedures
 - Company-wide and specific to function
 - Should be written



Step 5

- Train the work force
 - Sensitize
 - Impress personal responsibility
 - Obtain employee acknowledgement



Step 6

- Monitor compliance
 - Audit by privacy officer/committee
 - Document, document
 - Lesser penalties



Notification of Security Breaches

- Notification of security breach may be given
 - In writing
 - By telephone
 - Through Internet websites, email, and statewide media channels (in very limited circumstances)



Notification of Security Breaches

- The Attorney General's office
- All consumer reporting agencies



Contents of Security Breach Notice

- Notice of a security breach must include a description of:
 1. The incident in general terms
 2. The type of information subject to unauthorized disclosure



Contents of Security Breach Notice

3. Steps taken/to be taken by the business to protect personal information from further unauthorized access
4. A telephone number to call for further assistance
5. Advice to the person to remain vigilant monitoring for illegal activity



Other Provisions of ITPA

- Security freezes on credit reports
- Notice regarding rights to obtain a security freeze any time FCRA summary of rights required



Cybersecurity



SMITH MOORE LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP All Rights Reserved

Cybersecurity Breaches

- I. OVERVIEW
- II. EXAMPLES
- III. LAWS
- IV. CYBERSECURITY INSURANCE

SMITH MOORE LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP All Rights Reserved

Overview

- Importance
- Security Breach v. Security Violation
- Terms often used interchangeably

SMITH MOORE LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP All Rights Reserved

Overview

- Sectors Affected (2002-2010)*

- # 1 - Business
- # 2 - Healthcare
- # 3 - Education
- # 4 - Government

* Info. from datalossdb.org



Overview

- Types of Data Breached (2002-2010)*

- # 1 – Names and/or addresses
- # 2 – Social Security Number
- # 3 – Tie: Date of Birth and Credit Card Numbers
- # 4 – Healthcare information

* Info. from datalossdb.org



Overview

- Nature of Breach (2002 – 2010)*

- # 1 – External
- # 2 – Internal (Accident)
- # 3 – Internal (Intentional)

* Info. from datalossdb.org



Overview

- Types of Breaches*

- # 1 – Stolen Laptop
- # 2 – Hackers
- # 3 – Via the Web
- # 4 – Fraud

* Info. from datalossdb.org



SMITHMOORE LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP All Rights Reserved

Overview

- Costs Associated with a Data Breach

- \$6.75 Million
 - Average cost per incident of a data breach in the United States (2009)
- \$2.25 Million
 - Increase in average cost of a data breach between 2005 and 2008
- \$4.6 Million
 - Average loss in business per data breach (2008)

SMITHMOORE LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP All Rights Reserved

Examples

- Heartland Payment Systems Breach

- January 20, 2009
- Hacker
- 130,000,000 records
- Direct Costs: \$68,198,380.00

SMITHMOORE LEATHERWOOD
© 2011 Smith Moore Leatherwood LLP All Rights Reserved

Examples

- TJX Companies Inc.
 - January 17, 2007
 - Hacker
 - 94,000,000 Records
 - Direct Costs: \$64,113,000



Laws

- Health Care Sector
 - HIPAA and HITECH Act
- Identity Theft Red Flags Rule
- Federal (General Applicability)
- State



Insurance

- Increasing in prevalence
- Not covered under existing insurance policies
- Flexible



Insurance

- Policy Features
 - Direct losses
 - Notification expenses
 - Litigation and Regulatory Procedures
 - PR and Crisis Management Services





Presented by:



Julie C. Theall
704.384.2656



Frankie T. Jones, Jr.
336.378.5256