

Name: _____

Phone: _____

Health Care Section Forum

Best Practices for Protecting Sensitive Personal Information

Thomas M. Kernan, J.D., CHP
DAVIN Healthcare Solutions
tkernan@statstaffpro.com
statstaffpro.com

Mike Zinni
DAVIN Healthcare Solutions
mzinni@statstaffpro.com
statstaffpro.com

Tuesday, Oct. 25
4–5:15 p.m.



Health Care Section Forum

Best Practices for Protecting Sensitive Personal Information

<p>Tom Kernan, CHP Vice President of Strategic Planning and General Counsel DAVIN Healthcare Solutions</p>	<p>Mike Zinni Director of Software Development DAVIN Healthcare Solutions</p>
--	---

Tuesday, Oct. 25, 4–5:15 p.m.






**DAVIN
HEALTHCARE
SOLUTIONS**

Through collaboration and innovation,
we create technology that turns
healthcare workforce challenges into
opportunities that drive change

www.DavinHealthcare.com
@DavinHealthcare
Booth #1317



Thomas Kernan, Esq.
*Vice President
& General Counsel*

- J.D., summa cum laude, Albany Law School, 2003
- Member of the New York State Bar Association (Corporate Counsel, Labor and Employment Law and Health Law sections)
- American Staffing Association Health Care Policy Council Member
- Member of the International Association of Privacy Professionals
- Clerked at the New York Court of Appeals, 2003-2005
- Engaged in the private practice of law, 2005-2015
- Works with hospitals, care providers, and staffing vendors to maintain compliance and bridge the gap between state and federal policies and the needs of healthcare clients
- A diehard Detroit Tigers baseball fan
- Lives in Malta, NY with his wife, Renee, and two rambunctious sons

The personal information we collect

- SSN
- Home addresses
- Email addresses
- Licensing and certification records
- Employee medical records
- Employment history



Why we need to protect it


This information could be used to steal an employee's identity or commit any number of fraudulent acts

The government data breach

During the summer of 2015, the U.S. Office of Personnel Management ("OPM") discovered that security clearance data that included Social Security numbers, addresses, financial records, employment history, and fingerprints of an estimated 21.5 million individuals had been compromised.

The OPM Data Breach, the largest data breach ever reported by the federal government, is a stark reminder that employee information gathered as part of a credentialing or background check process is very much a target of cybercriminals.

The US has no unified set of laws governing information privacy and data security



HIPAA provides an excellent example of the gaps inherent in the sectoral approach to privacy and data security

*Data security requirements under HIPAA:
The privacy rule*

Implement administrative, physical and technical safeguards to protect the confidentiality and integrity of all PHI regardless of the form in which it is stored.

*Data security requirements under HIPAA:
The security rule*

Protect against reasonably anticipated threats and hazards to the security and integrity of e-PHI

Mandates that ePHI remain secure at all times, both at rest and in transit

HIPAA's Reach Does Not Extend to Staffing Organizations

It is a common misconception that HIPAA protects all medical records. In fact, the Privacy Rule and the Security Rule apply only to "covered entities" -- a term that includes health plans, healthcare clearinghouses and healthcare providers -- and to the business associates of covered entities.

Healthcare staffing organizations are in the business of recruiting, credentialing and assigning their employees to client health care institutions under whose direction and control the assigned employees perform their work. Inasmuch as health care staffing organizations do not directly provide patient care, they do not constitute covered entities. Further, inasmuch as the assigned employees of healthcare staffing organizations are generally treated as members of the client health care facility's workforce or acting in the capacity as members of the client healthcare facility's workforce, neither the assigned employees nor the health care staffing organizations are considered business associates.

As employers, health care staffing organizations are not required to comply with HIPAA regulations with respect to employee medical records gathered as part of the credentialing process. Indeed, HIPAA affords no protection whatsoever to employee medical records held by companies in their capacity as employers even though such records would be protected if held by such employees' insurance carriers or health care providers.

Section 5 of the FTC Act (15 U.S.C. § 45) prohibits “unfair or deceptive acts or practices in or affecting commerce.”

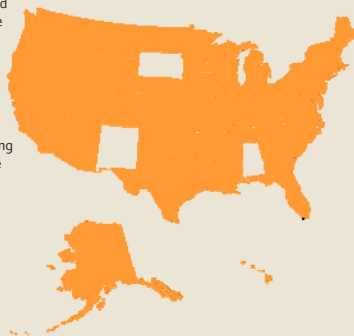
The failure to employ reasonable and appropriate measures to protect personal information against unauthorized access is itself an unfair act or practice in violation of section 5(a) of the FTC Act (15 U.S.C. § 45[a]).

Lax data security practices not only violate industry norms but may violate section 5 of the FTC Act

Unsafe practices include:

- ✘ Collecting personal information that is not needed or retaining personal information that is no longer needed for a legitimate business purpose
- ✘ Failing to restrict employee access to personal information based on business need
- ✘ Transmitting personal information in plain text
- ✘ Failing to require strong passwords and to periodically update them
- ✘ Failing to maintain current antivirus/malware protection software on workstations
- ✘ Failure to encrypt and secure laptops and portable hard drives

47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information.



States Have Taken a More Comprehensive Approach to Data Security

State data breach notification statutes may have extraterritorial application. Some states have enacted comprehensive data security standards that not only provide for notification in the event of a breach but also establish concrete technical standards.

*Case in Point:
The Massachusetts Data Security Regulation*



The Massachusetts Data Security Regulation (201 C.M.R. 17.00) establishes rigorous and far-reaching information security requirements, including the requirement that all companies that possess personal information of Massachusetts residents adopt a written information security program (WISP).

A WISP identifies and evaluates foreseeable risks to the security of personal information of Massachusetts residents. The Massachusetts Regulation expressly applies to all companies, regardless of where they are located, that possess personal information of Massachusetts residents.

* Whether you're a health care staffing organization, managed service provider, vendor management software provider, or health care facility that utilizes supplemental staffing, *you are responsible for the personal information you collect.*

<p>Health care workers possess a reasonable expectation that their personal information will be handled with care whether it is in the possession of their primary care provider, health insurance carrier or employer.</p>	<p>The failure to take appropriate measures to protect personal information may violate one or more state data security laws irrespective of whether a breach occurs.</p>	<p>Health care staffing organizations and managed service providers who fail to take such measures may be found to be engaged in an unfair act or practice affecting commerce, in violation of section 5(a) of the FTC Act.</p>
<p>In the event of a data breach flowing from shoddy data security practices, a company will not only be required to notify affected employees of the breach, but also navigate a potential minefield of conflicting state data breach notification laws.</p>	<p>Data breaches can cause significant reputational harm.</p>	<p>A number of states, including California, grant affected individuals the right to sue for harm suffered as a result of data breaches caused by the failure to adopt reasonable security procedures and practices.</p>

The cost of a breach

Based on the results of its recent study involving 64 companies across 16 industry sectors, the Ponemon Institute estimates that the average total cost of a data breach exceeded **\$7 million**.

The average cost per lost or stolen record was \$221. The average breach involved just over 29,600 records. Mega-breaches, those involving in excess of 100,000 records, generally cost substantially more.

Via Ponemon Institute, 2016 Cost of Data Breach Study: United States, June 2016
Study sponsored by IBM

Companies that fail to adopt reasonable data security policies, and take steps to educate their workforce about the importance of data security, risk serious adverse consequences for both the individuals whose personal information is placed at risk and their own bottom line.



Good data security practices are good business and should be a priority for every organization that handles sensitive personal information.



Michael Zinni
Director of Software Development

- Spent the first twenty years of his career working in large software groups for fortune 100 corporations developing mission-critical process automation software for manufacturing
- Founded his own software company, Zincastle, in 1999 and began developing custom desktop software and web-based applications for a wide variety of clients
- Each system Mike builds has a focus on security and usability
- When he's not writing code, he can be found in his garden, cooking, playing golf or riding his bicycle in Saratoga Springs, NY with his wife Cheryl

We are responsible for the information that we keep



We must make our best effort to protect that information

Why is hacking and Identity theft prevalent? > It's profitable



\$81 million

taken by romance scammers who target people on online dating sites by feigning love and then asking for money

\$12,000 per victim



\$51 million

taken by auto scammers, who convince their targets to pay for cars that don't exist

\$3,600 per victim



\$18 million

in real estate rental scams which, like auto scams, attempt to convince buyers to pay for property that doesn't exist

\$1,800 per victim



\$6 million

taken by FBI scammers, who pretend to be government officials to intimidate and extort money

\$700 per victim

via www.fbi.gov/cyber

Identity packages

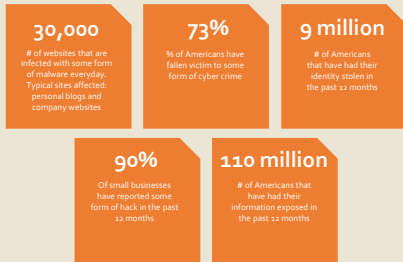
A dossier of packaged credentials for an individual that can be used to commit fraud

SSN + Email Address	As low as \$12.50
Credit Cards	\$15-\$30
SSN + Driver's License + Utility Bill	\$90
Physical Counterfeit SSN Card	\$140-\$250
Physical US Passport	\$3,000-\$10,000

What do hackers want?

Identity packages
Access to money
bank information, credit card information, etc.
Corporate Information

Launching point for other activities
Storage for stolen information
Network access to other computers

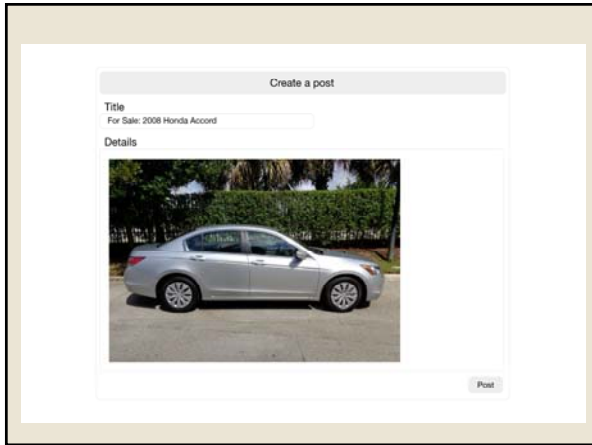


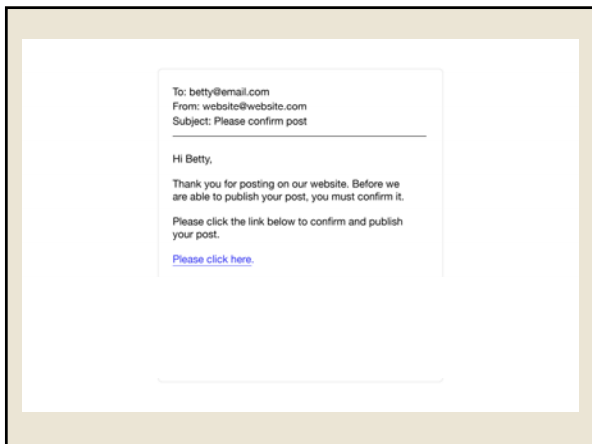
How do hackers obtain access?

Malware and viruses distributed through email and websites
Rogue networks masquerading as legitimate networks
Stolen and recycled devices
Insider access – employees, vendors
Through "legitimate applications"
Purchased services



The Anatomy of a Scam



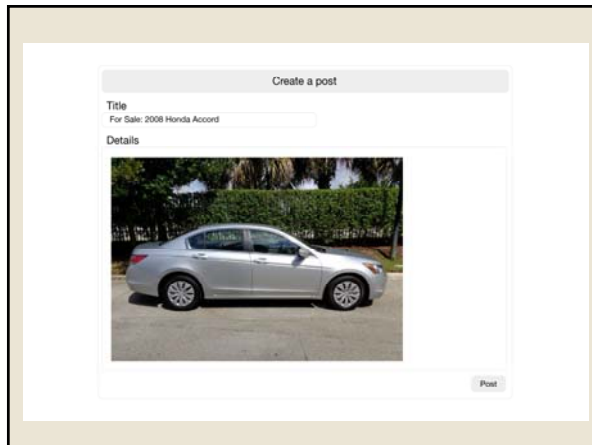


The screenshot shows a user interface with two main sections. The top section is titled "Log in" and contains two input fields: "Email / Handle" and "Password". Below these fields are two links: "Forgot Password?" and "Log in". The bottom section is titled "Create account" and contains an "Email" input field, a link for "Account help", and a "Create account" button.

The screenshot shows an email confirmation message. The header includes: "To: betty@email.com", "From: website@website.com", and "Subject: Thank you for confirming". The body of the email says: "Hi Betty, Thank you for confirming your post. Before we are able to publish it, we require a nominal fee per post. Please click the link below to be directed to our payment processing page." Below this text is a blue hyperlink that says "Please click here."

The screenshot shows a "Submit payment" form. It includes input fields for "Name", "Address", "City", "State", and "Zip code". Below these is another "Address" field. The payment method section features logos for VISA, MasterCard, American Express, and Discover, followed by a "Credit card number" field. There are also fields for "CSV" and "Exp. date". At the bottom, there is a "Billing information" section with a radio button selected for "Same as above" and a "Submit" button.

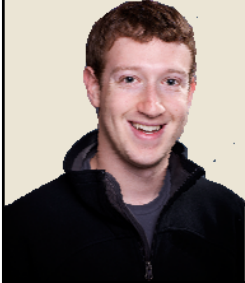
What just happened?



What can I find?

Personal Information		Bank Information	
Name	Physical Attributes	Credit Cards	Bank Statements
Address	Family Members	Income	Credit History
SSN	Pets		
DOB	Hobbies & Interests		
Work History	Health Information	Online & Offline Shopping Habits	

100 million LinkedIn passwords were published in May 2016



Do you use the same Passwords to access multiple applications and websites?

Apparently Mark Zuckerberg does: His published LinkedIn password was reportedly used to access his Twitter and Instagram accounts

Personal & Employee Security Audit

- +1 Every device has a unique user name and password to access
- +1 Every email account has a unique password
- +1 Unique passwords for all network connections VPN, mapped drives, remote desktops
- +1 Operating system is current and updates applied
- +1 Virus and malware protection subscription is current with updates
- +1 Rolling backups regularly created and tested
- 1 Files containing passwords on your computer?
- 1 Allow other applications to login with your social media or email credentials? (i.e. "login with your Facebook account")?

What is your score?

- 6 Well versed – the right approach
- 4-5 Close but not safe
- 2-3 Work to do
- Less than 2 Unplug!

Company Security Audit

- ✔ Does everyone pass the personal security audit?
- ✔ What sensitive information is being collected?
- ✔ Where is the sensitive information being stored?
- ✔ Who has access and why?
- ✔ How long is it stored?
- ✔ Non-administrative privileges for local computers
- ✔ A secure email is used
- ✔ Audit all applications installed/used

Applications Audit

- ✔ Cloud-based vs. desktop-based
- ✔ Vendor reputation
- ✔ Ask questions of your vendor

Recommendations

WISP – Written Information Security Plan

Risk assessment

Security Awareness Training

Regular reviews of WISP, risk assessment, and training

Use encrypted email or use a secure web portal to
Transmit sensitive information

Require users to have strong passwords and to regularly
change their passwords



Criminal enterprises exist with specialist operating all over the world

Processes, training, and technology in place to protect assets

Only as safe as the weakest link

Thank You for Attending



Tom Kernan, CHP
Vice President of Strategic Planning and General Counsel
DAVIN Healthcare Solutions



Mike Zinni
Director of Software Development
DAVIN Healthcare Solutions