

NAGDCA ANNUAL CONFERENCE 2009

Be sure to sign the
"Sign-In/Sign-Out" sheet
outside of the room when applying for
Continuing Education Credits
for the following certifications.
(Check the appropriate certification)

- CFP
- CPE

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Privacy and Security

Moderator:
Doug Miller, Suffolk County (NY)

Speakers:
Steve Farley, Nationwide Retirement Solutions, Inc
Richard Girardo, The Segal Company
Doug Miller, Suffolk County (NY)

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Privacy and Security

CONSIDERATIONS FOR GOVERNMENT DC PLANS

DOUG MILLER
DIRECTOR OF MANAGEMENT INFORMATION
SUFFOLK COUNTY NEW YORK

NAGDCA

Plan Administration

- Participants' Information
- Payroll Systems
- Providers Systems & Participants Data
- Personal Information
- Records Retention
- Public Safety Personnel



Internal Records

- Ensure Access and Identity management is in place
- Review access rights to Personal information
- Inventory Personal information sources
- Implement Monitoring tools
- Safeguarding mobile data



Provider Systems

- RFP Considerations
- Non- Disclosure agreements
 - Use of Third parties for systems maintenance
 - Record Keeping
 - Hardware Platforms
 - Software systems
 - Compatibility
 - Upgrades
 - Downtime
 - Conversions
 - Data
 - Disaster Recovery
 - Location of data center/s



NAGDCA ANNUAL CONFERENCE 2009

Continued

- Elements of Provider Disaster Recovery Plan
 - How often does the provider test the recovery plan?
 - How the provider handles:
 - System failures
 - Loss of power
 - Loss of backups
 - Testing
 - Outages

Austin © Waco San Antonio

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Plan Historical Data

- Telecommunications
 - Voice systems, VOIP Data
- Email retention
- Management reports
- Internet transactions
- UFE

Austin © Waco San Antonio

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Security

- Physical security
 - Access to data center
 - Safeguarding of facility
 - Access control system
- Authorized access to data
 - Background checks
 - Spot checks
 - monitoring
- Confidentiality of data
- Security for hard copy data
 - Shredding
- Information Retention policy
- Auditing
 - External audits
 - Penetration audits


Austin © Waco San Antonio

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Identity theft


- Stolen mail and trash (Curbside recycling)
 - Bank statements
 - Credit card statements
 - Tax information
 - Pay stubs
 - Stolen trash
- Theft (Old Fashioned Way)
 - Stolen Wallets and purses
 - Laptops, PDA, Computers, Cell Phones
- Other Ways:
 - Dishonest employees that have access to records.
 - Information divulged by you.
 - Information "hacked" from a business or website.
 - Email, instant messages, or websites that trick people into providing personal information



NAGDCA ANNUAL CONFERENCE 2009

Pitfalls of Privacy breaches


- Fines/Penalties
- Potential Lawsuits
 - Appearing in Federal Court
- Negative Publicity
- Low participation



NAGDCA ANNUAL CONFERENCE 2009

Additional information on the use of Social Security Numbers

- As a result of an increased problem with identify theft in the U.S., Congress made identity theft a federal crime in 1998. In order to further reduce opportunities for and the likelihood of identity theft, the Privacy Act of 2003 was introduced to set boundaries for the use of Social Security numbers. Other legislation is also pending to further restrict the sale, purchase and display of Social Security numbers. Although employee benefit plans are not required to safeguard Social Security numbers specifically, plan sponsors should implement policies and procedures to minimize the use of Social Security numbers when displaying, accessing or collecting information.
: Privacy Act of 2003



Social Security Numbers cont..

- Many states have enacted privacy legislation, complicating the picture for firms with operations in multiple states. Employers should establish formal policies addressing use of social security numbers as identification, restricting access and influencing vendors to follow suit. If the data must be used, it can be encrypted or limited to only the last four digits. Policies should address not only external use of social security numbers but also internal use, and there should be a response plan for an unauthorized disclosure of this valuable data



Personal information

- Since the 1970s there have been concerns about the collection, storage and use of personal information. Many states have some regulations on using Social Security numbers, but only California, Nebraska and Michigan address ways employers can handle and use the data. Michigan's Social Security Number Privacy Act may serve as a model for other states on disclosure, access and record maintenance and disposal, as well as penalties for violation. Employers should proactively establish policies and procedures on Social Security numbers as confidential data and ensure that third party providers ascribe to the procedures. The information on how such personal information may and may not be used should be published in employee handbooks.





Steve Farley
Vice President, Information Technology
Nationwide Retirement Solutions



NAGDCA ANNUAL CONFERENCE 2009

Information Security Risk Posture

- We work in highly regulated industry
- Data theft has become a daily story in the news
- Participant confidence is key
- Any lapse in information security could destroy confidence and result in hefty regulatory fines
- Could result in reputation damage for plan administrators and plan providers

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Information Risk Management Components

Information Risk Management (IRM) - The business of providing strategically focused and cost-effective management of information risk and assuring the **confidentiality, integrity, and availability** of plan sponsor and participant information assets

Information Security - The processes that provide protection of information assets stored by plan providers

Continuity Management - The primary purpose of ensuring plan providers can provide business and technology services in the event of a business interruption.

Records Retention - The practice of managing the regulatory and contractual requirements for storage and retrieval of information assets

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

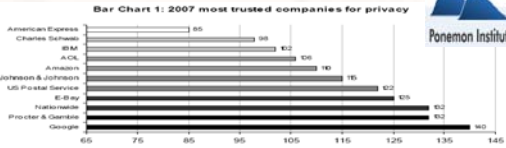
Information Security Responsibilities

- Protect confidentiality of plan sponsor and participant information
- Identify and maintain up-to-date ranking of the top risks facing our industry
- Work together to ensure the security, confidentiality and availability of our systems are aligned with regulatory and entity expectations
- Accurately measure and monitor overall acceptable risk posture levels
- Effectively identify and respond to the ever-changing risk landscape
- Ensure the availability of systems that manage transactions, data, and information on behalf of Plan Sponsors and Associates
- Manage and protect against malicious attacks on data

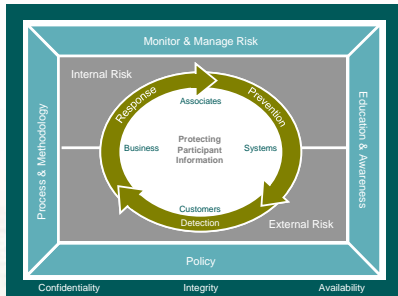
NAGDCA

Information Security Participant Trust

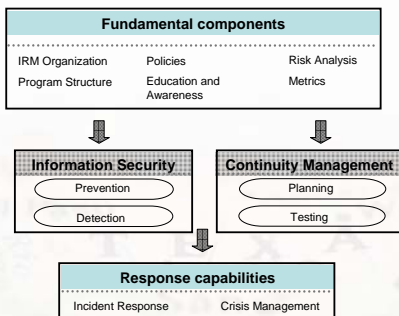
- Our participants expect that we keep their information private
- Privacy and trust are key business drivers. Providers and administrators must mitigate risk exposures in order to keep the trust of participants and live up to our commitments
- Per study by Carnegie Mellon University, Consumers will pay more online when privacy protections are strong.*
- The most Trusted Companies for Privacy in the 2007 TRUSTe and Ponemon Institute's Web-based research study....



Information Risk Framework




Information Security Practices



NAGDCA ANNUAL CONFERENCE 2009

Information Security Services



- Risk Management
 - Certification of provider systems and risk assessments
 - Attack & Penetration testing, and external 3rd party reviews
 - Education and Awareness
 - Consult with Plan Sponsors and Administrators
 - Implement pervasive solutions (laptop encryption, anti-virus software, etc.)
- Incident Handling and Response
 - Manage and facilitate information security incidents and events
 - Manage and close risk issues
 - Risk reporting including communication and informing of Plan Sponsors and Participants



NAGDCA ANNUAL CONFERENCE 2009

Continuity Management



In our effort to provide continuous service operations, both providers and administrators must develop a comprehensive Continuity Management program to include business recovery, systems recovery, and crisis management

NAGDCA ANNUAL CONFERENCE 2009

Continuity Management Program Services

- ✓ Establishment of policies and standards
- ✓ Consistency and consulting for Plan Sponsors
- ✓ Evaluation of crisis situations
- ✓ Activation of recovery plans
- ✓ Coordination of disaster response
- ✓ Oversee recovery plan development
- ✓ Organize regular recovery plan exercises
- ✓ Provide governance for compliance to policies

NAGDCA ANNUAL CONFERENCE 2009

Recovery Planning, Maintenance & Exercising

Recovery exercise requirements are determined by criticality of the business processes

- Business and systems recovery plans should be documented using industry tools
- Recovery personnel data updated regularly
- Recovery plans maintained in partnership with business and systems experts to ensure accurate and meaningful information

Recovery exercise frequency is driven by criticality of the recovery plan but most often annually

- Recovery plan reviewed and scored regularly
- Systems and disaster recovery exercises executed
- Business recovery or walk through exercises executed
- Activation/Notification exercises executed

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Records Retention Best Practices

- Embed records management compliance into our plan provider responsibilities
- Oversee a viable and visible records management process
- Maintain and educate on records management policies
- Audit and report compliance of policy and procedures
- Test and monitoring compliance
- Records management is dull and usually an afterthought. What are we doing to create a compelling call to action?

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Records Retention Practices

- Policy, Procedures and Retention Programs
 - Does your provider have a robust program that ensures compliance with records policy and procedures?
 - Do they have clear, legally defensible and actionable documents that explain the procedures and processes?
- Electronic Business Records
 - What are the official electronic record keeping systems being used?
 - Are they applying proper retention to these systems?
 - What about the rest of the "stuff" (emails, instant messages, text messages, blogs, wikis, Yammer posts, etc.)
 - Have they educated you on how the policies are enforced?
- Physical Records
 - How are they managing on-site and off-site physical records storage?
 - Have they properly addressed shredding requirements and provided associates the tools and knowledge to dispose of information properly?

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Emerging Trends

- The explosion of social media and the creation of records on assets that do not belong to administrators and plan providers. In other words, what responsibility do we have to manage records or communications that exist on Yammer, Facebook, LinkedIn, Gmail and on the cell phones that belong to participants or plan sponsors?
- The financial services regulatory structure is about to change dramatically. In other words, what will be our record keeping obligations in a post bailout world?

Austin
San Antonio
NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

A Brief Look at Compliance and HIPAA

Richard Girardo
The Segal Company

Privacy
Ctrl
NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Privacy and Security

- Key Points to Know about HIPPA
- Security
- Areas to Think About and *CORRECT*

El Paso
Waco
SOUTH TEXAS
Austin
San Antonio
NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

HIPAA

Health Insurance Portability and Accountability Act

Administration Overview

- HIPAA Electronic Data Interchange (EDI)
 - The standardized electronic transmission of health care data
- HIPAA Privacy
 - The protection of health care information that is spoken or written.
- HIPAA Security
 - The protection of electronic health care information; email, internet, etc.

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

What is EDI?

- Electronic Data Interchange (EDI) refers to the electronic exchange (sharing) of health information in a standardized format (transaction) between two or more covered entities

The EDI Rule: When 2 covered entities want to communicate electronically about certain health related matters such as billing, precertification, EOBs, or eligibility, their electronic communication must meet the federal HIPAA EDI electronic data requirements for format and content

NAGDCA

NAGDCA ANNUAL CONFERENCE 2009

Quick View of HIPAA

- Requires covered entities (health care providers, health plans and clearinghouses) to implement reasonable policies and procedures to protect individually identifiable health information (IIHI)
- Gives individuals the right to control access and disclosure of their individually identifiable health information
- Under HIPAA, a Business Associate (BA) is a person or vendor who performs a function or activity involving the use/disclosure of "individually identifiable health information" on behalf of a covered entity. The individually identifiable health information disclosed to or used by a BA must be protected. (Typical BA Claims Administrator (TPA), COBRA Administrator, Attorney, Accountant, Auditor, Consultant/broker, PPO networks, FSA Administrator, Disease Management vendor, etc.)

This is by no means is a full explanation of HIPPA Regulations

NAGDCA



NAGDCA ANNUAL CONFERENCE 2009

Security

•HIPAA Security regulations do not regulate, and ePHI (electronic protected health information) is not:

- paper and paper faxes
- copy machine voice
- voice mail
- telephone communication

• Electronic data that moves within and outside the covered entity IS regulated

NAGDCA ANNUAL CONFERENCE 2009

Security's 5 Key Areas

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies, Procedures & Documentation



NAGDCA ANNUAL CONFERENCE 2009

Administrative Safeguards

- Risk analysis and risk management
- Assign security responsibility to a person
- Written policies/procedures
- Measures to secure ePHI
- Management of the conduct of the workforce
- Training of the workforce
- Incident reporting and sanction policy
- Contingency plan (data backup, disaster recovery)




NAGDCA ANNUAL CONFERENCE 2009

Physical Safeguards

- Facility access controls to prevent unauthorized physical access/tampering
 - Restrict user access to PHI based on need-to-know, contingency operations, physical security of the facility 24/7, access controls
- Workstation use and security
 - Servers, routers, laptops
- Device and media controls
 - Disposal, media re-use, accountability, data backup and storage


Protecting physical media requires more than a lock on a door. You need to control alternate routes of access as well: air vents, drop ceilings, windows, fire escapes, etc. can provide a point of access



NAGDCA ANNUAL CONFERENCE 2009

Technical Safeguards


- Access controls
 - Identify who has access and to what?, unique user ID, emergency access procedures, automatic logoff, encryption and decryption methods
- Audit controls
 - Do an audit
- Person or entity authentication
 - Verify identity and allow access to PHI by only authorized users
- Transmission security
 - Integrity controls and encryption



NAGDCA ANNUAL CONFERENCE 2009

Organizational Requirements and Policies, Procedures - Documentation

- Organizational Requirements
 - Business Associate must sign a contract assuring their electronic security
 - Plan Document to be amended to address that plan sponsor safeguards electronic PHI
- Policies, Procedures & Documentation
 - Create and maintain policies and procedures for safeguarding electronic PHI
 - Maintain documentation for the later of: 6 years from the date of the electronic PHI creation or the date the electronic PHI last in effect.



Security for Handheld Devices

- Assure that available critical patches and upgrades are promptly applied
- Eliminate or disable unnecessary services/applications
- Configure user authentication and access controls
- Install content encryption, remote content erasure, firewall, antivirus, intrusion detection, anti-spam and virtual private network software
- Perform security testing



NAGDCA

Areas to Think About and Correct

- ePHI on computer monitor visible by anyone who comes into covered entity's office ("shoulder surfing")
- Access to network turned off but applications exist behind the operating system allowing unauthorized individuals to log into them
- Employees share workstations & access ePHI without a password
- Computers not shut down at end of day
- Backup tapes with ePHI not stored in secure location
- ePHI sent over Internet unsecured/unencrypted
- Employees throw-out floppy/discs into regular trash can
- No smoke detector/fire extinguisher or air conditioner paging warning system in room where server stored
- Computer equipment not plugged into a surge protector/uninterruptible power source
- Changing password is not required every so often
- HR and IT Departments don't communicate effectively so it takes days/weeks/months to terminate computer access by terminated employees, temps, auditors

NAGDCA

Areas to Think About and Correct

- No or few security policies and procedures
- User ID and Password on post-it note next to computer
- Using same password for multiple employees; Password never expires; Temporary employees use regular employee passwords
- ePHI residing on server on an external network
- Web server residing outside network firewall
- Servers stored in a room with window AC unit
- Server in locked room but accessible via ceiling tile
- Room where phone lines enter building not locked
- Laptop stolen...hard drive full of ePHI
- Staff use instant messaging bypassing e-mail controls
- ePHI stored in handheld devices easy to steal/lose, data not password protected
- Wireless not secure, not monitored for inappropriate access and not restricted to employees who really need it

NAGDCA

