HITCh at HIMSS 2008
The State Role in Health Information Technology

Tuesday, February 26, 2008
Speakers

- Christopher B. Sullivan, Ph.D.
  Administrator
  Agency for Health Care Administration
  Florida Center for Health Information and Policy Analysis
  850-414-5421 | sullivac@ahca.myflorida.com

- Senator Bob Hagedorn, Colorado

- Lory Wood
  Vice President
  Chief Security and Compliance Officer
  Good Health Network
  407-629-0304 | wood@ghnetwork.com
Florida’s Initiative to Empower Regional Health Information Organizations and Enable the Development of Health Information Exchange

National Conference of State Legislatures
Project HITCh at HIMSS

Orange County Convention Center
Orlando, Florida – February 26, 2008

Christopher B. Sullivan, Ph.D.
Agency for Health Care Administration
Florida’s Strategies for Empowering Regional Health Information Organizations

This talk addresses three areas in the development of health information exchange in Florida:

- A historical summary of the Florida Health Information Network (FHIN) initiative and Florida’s Regional Health Information Organizations (RHIOs).
- The current context of the Florida RHIOs in 2008 and their integration into the Florida Association of RHIOs.
- Florida’s ongoing strategies for developing the FHIN and its pursuit of initiatives to support RHIO sustainability.
The FHIN Begins at the Local Level

The Florida Health Information Network is being built from the local community up.

- AHCA’s strategic plan for promoting health information exchange is to empower local stakeholder collaborations focused on creating local health information networks.

- The FHIN is a collaboration of Regional Health Information Networks (RHIOs) funded by the FHIN Grants Program and by local in-kind support.

- Each RHIO is responsible for working with local providers to initiate the exchange of medical records through the RHIO portal.
The Florida Health Information Network

1. Big Bend Regional Healthcare Information Organization
2. Central Florida Regional Health Information Organization
3. Community Health Informatics Organization
4. North West Florida Regional Health Information Organization
5. Northeast Florida Health Information Consortium
6. Palm Beach County Community Health Alliance
7. South Florida Health Information Initiative
8. Tampa Bay Regional Health Information Organization

ahca.myflorida.com/dhit
Government Action Initiates the FHIN

The FHIN initiative began in 2004 with the Select Committee on Affordable Health Care for Floridians calling for “secure, private information sharing throughout health care.”

Governor Jeb Bush signed an Executive Order in May 2004, creating the Governor’s Health Information Infrastructure Advisory Board (GHIIBAB) “to promote the development and implementation of a Florida health information infrastructure.”
FHIN Strategy of AHCA and the Governor’s Advisory Board

Build out health information networks using a grants program to leverage the development of local RHIOs

Integrate the RHIOs with a state-level server that will manage data exchange among RHIOs and other state and federal databases

Create a not-for-profit organization to maintain the Florida Health Information Network and set standards of interoperability for the RHIOs
FHIN Grants Program Funding RHIOs

The FHIN Grants Program began in 2005 to empower local stakeholder collaborations focused on health information exchange.

All grants funds are matched dollar for dollar at the local level, indicative of a tremendous level of local passion and volunteerism.

Funding the FHIN Grants Program

The Florida Legislature has appropriated more than $5 million to fund the RHIOs through the FHIN Grants Program since 2005.

- $1.5 million in 2005
- $2.0 million in 2006
- $2.0 million in 2006

AHCA requested $6.8 million for the FHIN Grants Program in 2008-2009 to leverage ongoing RHIO development.
FHIN White Paper Addresses Core Issues

The FHIN White Paper addressed the core business operations of the network and the core services to be developed first.

- The FHIN was to facilitate communications and data exchange among providers and Regional Health Information Organizations to integrate statewide clinical health information exchange through a network architecture.

Blueprint for Building the FHIN

Blue Cross Blue Shield of Florida worked with AHCA to create a business plan for the FHIN.

- The BCBSF team created a revenue model that showed the FHIN becoming sustainable within five years if initial funding of $25.8 million over three years was appropriated by the Legislature.

- The business plan recommended that the FHIN make the critical data sets and infrastructure available for Florida’s RHIOs to establish their health information exchanges and develop products for revenue opportunities.
Outcomes of the FHIN Strategic Initiative

- The 2007 Legislature appropriated funds for the FHIN Grants Program only.
- The FHIN, Inc., bill did not pass.
- AHCA leadership began reevaluating the state level server strategy in favor of local projects.
- The Governor’s Health Information Infrastructure Advisory Board sunsets in June 2007.
- The FHIN Grants Program continued with no increase in funding.
- Strategic priorities of the FHIN are reconsidered.
PBCCHA All-Care Shared Health Record

- Real-time electronic interface to existing data systems used by hospitals, clinics, and other safety net providers.
- Shared summary records created for all uninsured/Medicaid/other patients.
- No duplicate data entry.
- Free clinics, Federally Qualified Health Centers, PBCCMS Project Access and key competitor safety net hospitals are participating.
- Viewable via the Web - after patients have signed authorizations.
Florida Agency for Health Care Administration
Florida Center for Health Information and Policy Analysis

NOTE: Views are limited to credentialed practitioners with patient authorization.
NEFHIC Technical Capacity

- ASP Model – Safety net data repository server hosted in Cerner’s secure datacenter with redundant hardware and power
- Records for 90,000 clients loaded with feeds from 7 participants, including hospitals and clinics
- System operational and accessible via the Internet using 128-bit secured communications
- Pilot testing of user access and data retrieval is complete
Big Bend RHIO

Florida Agency for Health Care Administration
Florida Center for Health Information and Policy Analysis

National Conference of State Legislatures Project HITCh at HIMSS
Current Big Bend RHIN Services

- Data Sharing – Patient demographic and clinical data feeds from major providers.
- RHIN Web Portal – Secure web interface for clinicians.
- User Access & Audit Control – Detailed audit logs across the entire system.
- Disaster Recovery & Business Continuity.
- Document Imaging
Florida Association of RHIOs (FAR)

Leaders of the Florida RHIOs created through the Florida FHIN Grants Program formed the Florida Association of RHIOs (FAR) in 2007 to:

- maximize their collective resources and
- promote use of electronic health information exchange across the state.

- FAR serves the collaborative interests of its members and the communities which they serve.
Rethinking Strategies for Fostering Statewide Health Information Exchange

- Continue the FHIN Grants Program
- Establish a Health Information Exchange Coordinating Committee for state level leadership.
- Work with the Health Information Security and Privacy Collaboration to reduce barriers to HIE.
- Ensure the sustainability of Florida’s RHIOs.
- Seek alternate funding sources to support RHIO development.
AHCA Creates the Health Information Exchange Coordinating Committee

- Will help establish a privacy-protected, secure and integrated statewide network for the exchange of electronic health records.
- Will provide technical guidance to RHIOs developing and operating health information exchanges in Florida.
- Will advise the Agency regarding developments in health information technology and national standards related to the security of electronic health information exchange.
Florida Health Information Security and Privacy Project

National Project intended to provide the Office of the National Coordinator of HIT with information about privacy and security practices and laws in 33 states that were part of the project.

- Each state identified business practices related to electronic health information exchange and analyzed practices and laws that are barriers to interoperability.
- The goal of the project was to develop state specific solutions and develop a plan for eliminating barriers to health information exchange.
Major Barriers to Health Information Exchange

- Inconsistent and fragmented laws at state and federal level – conflicts between Florida statutes and HIPAA.

- Lack of standard requirements for when to use patient consent – proposed uniform consent form.

- Mistrust among health care entities, liability concerns and fear of violating rules or litigation.

- Solution is to develop priority legislative recommendations for legislative action that would have the most immediate impact.
Health Information Security and Privacy Collaboration Legal Working Group

The HISPC Legal Working Group developed priority legislative recommendations.

- Reconcile hospital licensure statutes and medical practice statutes (s. 395.3025 FS).
- Reconcile clinical laboratory statutes and medical practice statutes (s. 483.181 FS).
- Develop a uniform consent process and establish patient consent requirements for RHIOs.
The HISPC Risk Self-Assessment Tool

There is a clear need for RHIOs to deal with security up front in developing their organizations.

- HISPC grant used to develop a risk self-assessment tool for RHIOs to address their security issues.
- Based on National Institute of Standards and Technology Security Standards.
eHI Value Sustainability Model

In 2007 eHealth Initiative worked with the Florida RHIOs to provide training in its Value and Sustainability Model.

One of the first steps in this tool is to define the list of HIE functionalities that your community will implement. eHI has asked a panel of experts to define a list of possible HIE functionalities, presented below. However, you may not find the specific function you are looking for on the list. Or, you may wish to combine several functions under a single label. If so, you may enter up to three of your own function labels in the yellow cells below.

<table>
<thead>
<tr>
<th>Standard List of HIE Functions</th>
<th>User-Defined Functions (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case management and care coordination</td>
<td>Enter User Defined Function #1</td>
</tr>
<tr>
<td>Claims management</td>
<td>Enter User Defined Function #2</td>
</tr>
<tr>
<td>Clinical document sharing</td>
<td>Enter User Defined Function #3</td>
</tr>
<tr>
<td>Health plan enrollment verification</td>
<td></td>
</tr>
<tr>
<td>Historical allergy list</td>
<td></td>
</tr>
<tr>
<td>Historical procedure list</td>
<td></td>
</tr>
<tr>
<td>Historical visit/hospitalization list</td>
<td></td>
</tr>
<tr>
<td>Medical record</td>
<td></td>
</tr>
<tr>
<td>Medication decision support (safety or other alerts)</td>
<td></td>
</tr>
</tbody>
</table>
eHI Value and Sustainability Model

- The Value and Sustainability Model employs a five step process:
  - Assess: Market readiness
  - Define: Decision framework
  - Evaluate: Net Present Value Model
  - Plan: Development of Business Plan
  - Execute: Acquire required starting capital, begin execution

- The Value and Sustainability Model addresses the challenges facing most RHIOs
Medicaid Claims-Based Electronic Health Record System Ported Through RHIOs

- Working with the new Medicaid fiscal agent, EDS, on a pilot project to roll out a claims-based EHR for Medicaid physicians.

- Medicaid pilot to work with Big Bend RHIO to integrate the claims data feed for display on the Big Bend portal.

- Plan to roll out the Medicaid EHR through RHIO portals in spring 2008.
Medicaid Claims-Based Electronic Health Record System Pilot

Medicaid-EDS Web Application

Local RHIO or Direct Medicaid Portal Access

Florida Agency for Health Care Administration
Florida Center for Health Information and Policy Analysis

HIMSS RHIO/HIE Symposium – 24 February 2008
Accessing Medicaid Prescription Data Through e-Prescribing with eMPOWERx

- The Florida Center is working with Gold Standard and Medicaid to make eMPOWERx medication history available to Medicaid physicians through RHIO portals.

- Florida Medicaid eMPOWERx e-prescribing software provides 100 days of a patient’s prescription drug history available to physicians.

- eMPOWERx uses clinical pharmacology report tools to alert the provider to potential drug-drug interactions.

- Providers can write prescriptions from a desktop computer to any pharmacy for dispensing.
Florida Medicaid Wireless Handheld PDA Project Approach

- Providers use eMPOWERx PDA (Windows Mobile 2003 Phone Edition) to access eMPOWERx Server (drug info, rx history and formulary).
- eMPOWERx Server connects to SureScripts for eRx services.
- SureScripts is associated with pharmacies for prescription fulfillment.

System Overview:
- Windows Server 2003, SQL 2000, IIS
- eMPOWERx Web site
Outcomes of the Medicaid e-Prescribing Pilot Project Using PDAs

- Prescribers who used eMPOWERx write 25% fewer prescriptions than physicians not using the system.
- Prescribers who use eMPOWERx save Florida Medicaid an average of $48 per patient per month on prescription claims.
- Florida Medicaid reports $1.8 - $2 million in monthly savings from electronic prescribing.
- During 2006, eMPOWERx users received more than 5,000 drug interaction alerts each week, more than 1,000 of which were of high or very high severity.
Average Monthly Cost Savings per Patient in Medicaid Wireless PDA Program

Average Prescription Cost per Patient

- Average PDA = $228
- Average Non-PDA = $276

Average Monthly Cost Savings per Patient in Medicaid Wireless PDA Program

Florida Agency for Health Care Administration
Florida Center for Health Information and Policy Analysis
FCC Telehealth Pilot Program

In November 2007 the Federal Communication Commission awarded $9.6 million to the Big Bend RHIO and AHCA to build a gigabit fiber network to nine rural hospitals and surrounding clinics in the Florida Panhandle.

- This contract will allow the Big Bend RHIO to connect these hospitals with gigabit fiber and extend its RHIN services to them.
- Providing broadband optical fiber connections to rural hospitals brings them into the Florida Health Information Network.
FCC Rural Broadband Pilot Project
Connecting Nine Rural Hospitals in the Florida Panhandle
Nationwide Network of Health Care Facilities

Symbology:
- Non-rural Facility
- Rural Facility
- National LambdaRail
- Internet2 Network
- Regional Networks
- Planned Networks
- National Capital
- State Capital
- City over 500,000
- City under 50,000
- County
- State / Territory
Work with the Florida Association of RHIOs (FAR)

- Develop policies and procedures and security and privacy standards with the RHIOs
- Foster savings in volume purchasing of HIT, network and data center services, and business operations
- Support standardization and interoperability of EHR systems and related interfaces
- Examine low cost open-source EHR solutions that can be installed in small physician practices and community clinics.
- Provide EHR adoption education and technical assistance to providers and practitioners
Next Steps for RHIO Sustainability

○ AHCA continues to work with the Legislature and the RHIOs across the state to create a viable approach to successful health information exchange.

○ Legislative appropriations for startup funding is still of great importance to the RHIOs.

○ Developing viable business models for the RHIOs is also essential for continued sustainability.

○ AHCA and the Florida Association of RHIOs must continue to work together on policy and technical issues of common interest.
Vision for the Florida Health Information Network (FHIN)

The vision for the Florida Health Information Network proposes integrating Florida’s community-based activity in clinical health information exchange through a statewide network, the FHIN.

• The FHIN will empower physicians to access timely and accurate medical records in order to deliver high quality medical care for their patients.
Good Health Network

Presentation to

Project HITCh

Tuesday, February 26, 2008
Presentation Summary

• Introduction to Problem
• Identify Issues and Concern
  - Data Breaches
  - Fraud
  - Medical Identity Theft
• HIPAA
• Security and Privacy Compliance
• Current Pending Legislation
• Recommendations
• Discussion and Questions
Defining the Problem

• The demand for privacy has lagged behind the rate at which data has been collected
• Lack of effort to develop appropriate security architecture into the health information technology to protect fraudulent misuse of consumer information
• Lack of reporting and enforcement of penalties when data breaches or misuse of information occurs
• Consumer notification of misuse of healthcare information is nonexistent
Definitions Overlap

• Data Breach
• Fraud
• Identity Theft
Data Breach Definition

A data breach occurs when unsecured personally identifying information held by an individual, company or government agency is mishandled, lost or stolen - resulting in confidential information falling into the wrong hands. Personally identifying information is most commonly defined as any data that links an individual's name with his or her Social Security, driver's license, financial account, medical or other confidential personal information.

-Cyber Security Industry Alliance
Fraud Definition

Intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right - Merriam Webster Dictionary

Fraud must be proved by showing that the defendant's actions involved five separate elements: (1) a false statement of a material fact, (2) knowledge on the part of the defendant that the statement is untrue, (3) intent on the part of the defendant to deceive the alleged victim, (4) justifiable reliance by the alleged victim on the statement, and (5) injury to the alleged victim as a result. - Legal-Dictionary
Identity Theft Definition

Identity theft is defined both by statute (ID Theft Act, 18 U.S.C. § 1028(a)(7), 1029(e)) and by FTC rule (16 C.F.R. § 603.2), and includes the misuse or attempted misuse of any identifying information – such as the SSN, biometric data, or an existing credit card account number - to commit fraud.

- FTC 2006 Identity Theft Survey Report
Impact of Financial Identity Theft

• Data breach incidents costs companies $197 per compromised customer record in 2007 compared to $182 in 2006.
• Lost business opportunity represented the most significant component of the cost increase, rising from $98 in 2006 to $128 in 2007.
• Individuals spend an average of 97 frustrating hours, with an average loss of $1,342, attempting to correct their files, scores and to clear their good name.
• "Our research clearly shows that data breaches are affecting consumers' trust in the organizations with which they share their data and ultimately, their buying behavior," says Dr. Ponemon.

1 Ponemon Study – Traverse City, Michigan – November 28, 2007
In the News

Medical identity theft

Many consumers take precautions against identity theft, but what about medical identity theft?

In addition to financial peril, victims can suffer physical danger if false entries in medical records lead to the wrong treatment.

"The crime occurs when someone uses a person's name and sometimes other parts of their identity -- such as insurance information -- without the person's knowledge or consent to obtain medical services or goods," said Launnda B. Haman, PhD, RHIA, associate professor and chair of the health information management department at Temple University's College of Health Professions.

"A person's identity information is valuable, too. This is not a common event," she says. She recommends consumers review the growing number of cases of medical identity theft online.

Persona non grata?

Despite their stake in the emerging national health information network, consumers are often overlooked by health IT planners.

BY JOHN BHADRA
Published on February 4, 2008

"You can get a lot of people on the list," says John P. Byrne, co-founder and president of Health Information Management Systems Society (HIMSS). "But that physician is Dr. Deborah Fox, a patient advocate who has been a vocal advocate for patients."

Gartner Voice

For business and IT professionals

Medical Identity Theft

Medical Identity Theft

Medical Identity Theft

"The definitions that are being used to compile these statistics are overbroad," he says. "I'm not saying it isn't a problem -- it's just a problem that the average person isn't likely to encounter. HIPAA has actually made dealing with such problems worse because people can't get their medical files corrected, which is just ridiculous."

In Dixon's opinion, "one person being victimized by medical identity theft is a problem and something we need to be concerned about."

Protecting yourself

Because HIPAA protections are riddled with loopholes, there is only so much you can do to protect yourself.
• Criteria and methods
  - Based on U.S. population age 18 and over of 222.94 million as of July 1, 2005
  - Study was conducted through telephone interviews using a Random-Digit-Dialing (RDD) sampling methodology
  - Total of 4,917 interviews were conducted between March 27 and June 11, 2006
Facts about Financial Identity Theft

- The median value of goods and services obtained by the identity thieves for all categories of ID theft was $500. Ten percent of victims reported that the thief obtained $6,000 or more, while 5 percent reported that the thief obtained at least $13,000 in goods and services.

- Where the identity thieves opened new accounts or committed other frauds, the median value of goods and services obtained by the thieves was $1,350. Ten percent of these victims reported that the thief obtained $15,000 or more in goods and services; in the top 5 percent, the thief obtained at least $30,000 in goods and services.

- 3.7% of respondents (3.0% - 4.6%) said they became aware of being a victim of ID theft during 2005. This suggests that 8.3 million American adults (6.6 million – 10.3 million) discovered they were ID theft victims in 2005.

In most cases, victims are not legally responsible for the cost of fraudulent transaction by identity thieves using their personal information. A variety of laws limit consumers’ liability in these situations. Such laws include the Truth in Lending Act, 15 U.S.C. § 1601 et seq., implemented by Regulation Z, 12 C.F.R. § 226; see especially 15 U.S.C. § 1643; 12 C.F.R. § 226.12(b) (limits consumer liability for unauthorized credit card charges to a maximum of $50), and the Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq., implemented by Regulation E, 12 C.F.R. § 205; see especially 15 U.S.C. § 1693g; 12 C.F.R. § 205.6(b) (limits consumer liability for unauthorized electronic fund transfers depending upon the timing of consumer notice to the applicable financial institution). Consumer liability for losses associated with checking account fraud and loan fraud are typically limited by state statute or common law, although consumers are sometimes held liable.


Copyright © 2007 Good Health Network, Inc.
Facts about Medical Identity Theft

• A total of 3.7 percent of survey participants indicated that they had discovered they were victims of ID theft in 2005. This result suggests that approximately 8.3 million U.S. adults discovered that they were victims of some form of ID theft in between 2001 and 2005.

• 0.8% of respondents (0.5% - 1.2%) fall into the category labeled “New Accounts & Other Frauds.” This category includes victims whose personal information had been used to obtain open new accounts or commit other frauds like receiving medical care. (1.8 million American adults)

• Three percent of these victims said the thief had obtained medical treatment, services, or supplies using their personal information (54,000 American adults)

Based on responses of people who discovered that their information was being misused in 2005, 20% of ID theft victims included having their personal information used in “Non-Account ID Theft,” 61% reported a specific way that their information had been misused and 18% had their information used by the thief to obtain medical treatment, services, or supplies.

Health Insurance Portability and Accountability Act (HIPAA)

- Requires usage of national standards for electronic health care information at the government and business level
  - Have a compliance official
  - Set standards of conduct into policies, procedures, or guidelines so that people know what the expected behavior is
  - Training and education of all staff on an ongoing basis, including additional training for specific employees
  - Incident reporting to correct and prevent incidents
  - Incident response procedures in the form of a plan and a team
  - Auditing and monitoring continually, with an evaluation and validation process set at regular intervals
  - Corrective actions applied consistently (sanctions, risk management, security controls)
HIPAA Rules Reviewed

Privacy
- Consumer Amendments (§164.526)
- Right to Restrict & Access (§164.522, §164.524)
- BAA (§164.308, §164.314)
- Consumer Mitigation (§164.530)
- Disclosure and Auditing (§164.528)
- HIPAA Training (§164.530)
- Limiting Data & Research (§164.514)
- Opt-in Marketing (§164.508)
- Privacy Policies (§164.316)
- Privacy Statement (§164.520)
- Consents and Authorizations (§164.506, §164.508, §164.510)
- User/Entity Directories (§164.510)

Security
- Security Management Process (§164.308)
- Assigned Security Responsibility (§164.308)
- Workforce Security (§164.308)
- Information Access Management (§164.308)
- Security Awareness and Training (§164.308)
- BAA (§164.308, §164.314)
- Facility Access Control (§164.310)
- Access and Audit Controls (§164.312)
- Transmission Security (§164.312)
- Documentation, Policies and Procedures (§164.316)
General Categories of HIPAA Security and Privacy Regulations

- Appropriate and reasonable safeguards
- Mapping PHI data flow
- Protecting appropriate data
- Access control
- Third party agreements
- Accountability
- Training and awareness

...Gaps Exist
Gaps in HIPAA Exist

- Individuals’ rights to correct errors in their medical histories and files need to be expanded to allow them to remove false information from their files.
- Guarantee an individual’s right to supplement, amend, correct, destroy and segregate any protected health information maintained or stored by an entity.
- Individuals should have the right to receive one free copy of their medical file.
- Individuals should have expanded rights to obtain an accounting of disclosures of their health information.
- Notification of medical data breaches to consumers has the potential to save lives, protect health, and prevent losses.
- Patient’s right to privately sue violators for violating their privacy rights.
- Prohibit the disclosure or use of health information without patient authorization for any purpose.
- Mandate that entities conduct annual risk assessment, management and control exercises to detect, prevent and limit security threats or breaches.
- Create an office of health information privacy within HHS with stricter penalties.
Models for the States

- DoD Information Assurance Certification and Accreditation Process (DIACAP)
  DoDI 8510.01
  http://iase.disa.mil/ditscap/

- NIST 800 Series - Special Publications in the computer security community
  http://csrc.nist.gov/publications/PubsSPs.html

- Healthcare Information Technology Standards Panel (HITSP) Security and Privacy Technical Committee
  HITSP/ TN900 - Security and Privacy V1.1
  - HITSP_v1.1_2007_TN900 - Security and Privacy
  - HITSP_v1.1_2007_C19 - Entity Identity Assertion
  - HITSP_v1.1_2007_C26 – Nonrepudiation of Origin
  - HITSP_v1.1_2007_T15 - Collect and Communicate Security Audit Trail
  - HITSP_v1.1_2007_T16 - Consistent Time
  - HITSP_v1.1_2007_T17 - Secured Communication Channel
  - HITSP_v1.1_2007_TP20 - Access Control
  - HITSP_v1.1_2007_TP30 - Manage Consent Directives
  - HITSP_v2.1_2007_TP13 - Manage Sharing of Documents
FTC Consumer Help

Take Charge: Fighting Back Against Identity Theft

APPENDIX

It's The Law

Federal Law


Under federal criminal law, identity theft takes place when someone "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Under this definition, a name or Social Security number is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

Violations of the federal crime are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Social Security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

For the purposes of the law, the FCRA defines identity theft to apply to consumers and businesses.

State Laws

Many states have passed laws making identity theft a crime or providing help in recovery from identity theft; others are considering such legislation. Where specific criminal identity theft laws do not exist, the practices may be prohibited under other laws. Contact your state Attorney General (for a list of state offices, visit www.naag.org) or local consumer protection agency for laws related to identity theft, or visit www.consumer.gov/idtheft.

Instructions for Completing the ID Theft Affidavit/ID Theft Affidavit [PDF only]

Annual Credit Report Request Form [PDF only]
Consumer Responsibilities

6 Ways to Protect Your Medical ID
Don't be a medical ID theft victim!
From Reader's Digest
November 2006

1. Treat your insurance card like a credit card. Don't lose it or loan it, and don't show it to anyone except a trusted health care provider.

2. Watch out for "freebies." Be suspicious of offers for free medical care. Avoid clinics that advertise aggressively, promise to waive co-payments, provide free transportation, or similarly entice you.

3. Read the EOB. Carefully review the "explanation of benefits" letters sent from your insurance company, and call about claims for services or drugs that you don't understand.

4. Check your benefits yearly. Once a year, request a listing of benefits paid out by your insurer. That way, you'll discover fraudulent payments even if the thief has changed your billing address.

5. Request an accounting of disclosures. You have a right under HIPAA to get this document from every health care provider you visit. The accounting will detail what personal information was released and whom it was sent to. It's a good way to catch and track theft, because any fraudulent medical information will probably be passed along to other providers.

6. Review your credit report. If someone has stolen your medical identity and racked up unpaid hospital bills in your name, the charges could turn up on your credit report.

For more information, go to worldprivacyforum.org and bcbs.com.
Compliant technology promotes interoperability and information exchange between all healthcare technologies securely:

- Identity proofing technology ensures the identity of all participating parties.
- Roles based access control will appropriately limit access to information to the appropriate parties and enable full transparent auditing.
- Nonrepudiation of origin and transactions will invoke trust.
- Secure communications will improve care.
- Consent and directives management allow appropriate sharing of information.
Security Risk Assessment

Four Authentication Assurance Levels for Multiple Risk Levels

Increased Complexity

Increased Identity Assurance

Authentication Factor Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Something you know</td>
<td>No Identity Validation (Website Registration)</td>
</tr>
<tr>
<td>II</td>
<td>Something you know, Something you have</td>
<td>Identity Proofing (1-9 Process)</td>
</tr>
<tr>
<td>III</td>
<td>Something you know, Something you have, Something you are</td>
<td>Risk Analytics (Lexis Nexis)</td>
</tr>
<tr>
<td>Multi</td>
<td>Something you know, Something you have, Something you are, Others</td>
<td>Security Clearance</td>
</tr>
</tbody>
</table>
Digital Identity Management

- Identity Proofing - Verifying the Digital Identities
- Roles Based Access Control
- Transparent Audit Trails
- Nonrepudiation of Origin and Transactions
- Secure Communications
- Consents and Directives Management
High Level of Identity Assurance

Two-Factor Authentication

**Something you know** is your password

**Something you have** is the digital certificate on your **Smartcard**

or **Security Token**
Current Legislative Considerations

- **Technologies for Restoring Users’ Security and Trust (TRUST) in Health Information Act** would provide grants and establish a standards-setting process to foster a nationwide health information exchange network. But the TRUST bill differs from the others by calling for:
  - An opt-in system that would require patient consent before records could be kept in electronic system.
  - Mandatory notification of any privacy breaches in health IT systems
  - Requirements for encrypting data and taking other security measures to protect records from unauthorized access.

- **Promoting Health IT Act** holds tremendous promise for improving patient care, reducing medical errors and lowering costs

- **Electronic Health Information Privacy Act** closes HIPAA’s most obvious gaps, including restoring the right of patient consent, strengthening enforcement, and providing audit trails and other technology remedies that improve patients’ ability to control their information

- **Health Information Privacy and Security Act of 2007** will give patients more control over their protected health information and create a private right to sue violators
Recommendations

1. Parallel legislation as the Fair Credit Reporting Act for victims of Medical ID Theft
2. New harsher laws for healthcare fraud similar to the drug dealer legislation
3. Need Business Intelligence and Predictive Analytics in place from the beginning of the NHIN to identify potential trends in breaches and fraud similar to the financial industry
4. Open transparent auditing logs viewable by consumers allowing early intervention when mistakes or fraud occur
5. Better accounting when providers disclose medical information to other providers which will be a key way to track down and correct mistakes
6. Insurance card issued with photos and signatures
7. HIPAA should be amended to allow patients the right to correct errors or even prevent errors from being passed along to other providers to prevent potentially fatal situations
8. Roles Based Access Control (RBAC) to limit healthcare staff access to only the information they need to perform their duties and alerts when inappropriate access is attempted
9. All covered entities should be required to perform internal risk assessments to prevent security breaches
The Best Healthcare System in the World deserves the “best of breed” technological solutions…..

We can do it together!
Open Discussion

Thank You

Contact Information

Lory Wood
Vice President
Chief Security and Compliance Officer
Good Health Network
218 Jackson Street
Maitland, Florida 32751
407-629-0304
wood@ghnetwork.com
Any Questions

• Among the Panelists?

• From the audience?

• You can either
  • Unmute and ask as part of the call or
  • Use Q and A option in your web-assisted audioconference.

• After the call, email questions and suggestions for future web-conferences to:
  • Health.hitch@ncsl.org
To Follow Up

- Feel free to contact us for more information at Health.hitch@ncsl.org

- For more program information and related links, and to see past programs: http://www.ncsl.org/programs/health/webcast2.htm

- This program was recorded and will be made available on line.
Florida

- Agency for Health Care Administration HIT Page
  http://ahca.myflorida.com/dhit/index.shtml

- Florida Health Information Network
  http://www.fhin.net/index.shtml

- E-prescribing Clearinghouse
  http://www.fhin.net/eprescribe/Index.shtml

- E-prescribe Florida
  http://www.eprescribeflorida.com/
The State Alliance for e-Health
www.nga.org/center/ehealth

Health Information Protection Taskforce report to the State Alliance for e-Health
http://www.nga.org/Files/pdf/0708EHEALTHREPORT.PDF

Final HISPC reports Final HISPC reports
www.rti.org/hispc

Georgetown Health Privacy Project
http://www.healthprivacy.org/

HEALTH INFORMATION TECHNOLOGY: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy, January 2007, GAO.

Privacy, Security, and the Regional Health Information Organization. Rosenfeld, Koss and Siler, Avalere Health LLC June 2007, California Healthcare Foundation
Resources from NCSL

Related NCSL Projects

- **Health Information Technology Champions (HITCh)**
  The HITCh partnership serves state legislators interested in health information technology (HIT) and health information exchange (HIE).
  
  [http://www.hitchampions.org/](http://www.hitchampions.org/)

Other NCSL Resources

- **State Health Notes articles on Health Information Technology**

- Subscribe to our bi-weekly newsletter *State Health Notes*

---

Donna Folkemer  
Group Director  
Forum for State Health Policy Leadership  
**National Conference of State Legislatures**  
Tel: 202-624-8171 | donna.folkemer@ncsl.org  

Kory Mertz  
Research Analyst  
Forum for State Health Policy Leadership  
**National Conference of State Legislatures**  
Tel: 202-624-3580 | kory.mertz@ncsl.org  