



**The Changing Landscape  
of Personal Health Records  
and Protected Health Information**

*FMI Pharmacy Conference  
September 13, 2009*

## Agenda Topics

- Accelerating demand for Retail Pharmacy data in Healthcare I/T
- Latest clinical data uses for Retail Pharmacy data
- The unique requirements of Personal Health Records
- The challenging landscape of clinical data providers
- Impact of Privacy, Consent, HIPAA, and ARRA
- Key considerations for Retailers as they move to participate

## Speaker Background

- Surescripts provides a neutral national network that facilitates e-prescribing
  - We enable prescription benefit, prescription history, and prescription routing
  - We do not own, sell, or promote any end user solution to pharmacies or prescribers
  - We established and enforce the *Patient Choice of Pharmacy, Prescriber Choice of Therapy*, and the *No Commercial Messaging* requirements across the network
- Surescripts focus is on certification, quality, collaboration
  - We drive the development, usage, and enhancement of national standards, workflow enhancements, and quality Best Practices for e-prescribing
  - We ensure that all of the hundreds of software vendors across the network are compliant to a consistent set of technical, workflow, and business requirements
  - The company's leadership collaborates with and provides guidance to national, regional and state health IT initiatives
- Surescripts is the result of the 2008 merger of SureScripts and RxHub
  - We were founded and continue to be owned by the Pharmacy Industry (NACDS and NCPA) and major PBMs (CVS/Caremark, Express Scripts, and Medco).

## Clinical demand for Pharmacy data

### Drivers of the growth:

- Federal & State Government push for Healthcare I/T
  - Medicare Modernization Act
  - American Recovery & Reinvestment Act (ARRA)
- Regional Healthcare Collaboratives & Exchanges
  - Driven by Quality, Efficiency, Access, Competition, and Funding
- Modernization of Point of Care provider systems
  - Rapid increase of investment in technology
  - Widely expanded marketplace and providers
- Advancement in Clinical capabilities of I/T based solutions
  - Data driven solutions that improve patient care
  - Realization of data value and accessibility coming together

## The focus on Retail Pharmacy data

- Strong understanding of the clinical value of prescription data
  - Prescription therapy is the most widely used treatment by physicians....
    - ...but also the most widely under or misused by patients.
  - No reliable feedback loop to providers on the results of their prescribed therapy.
  - Ability to avoid interaction, duplication, intentional misuse hampered.
- Retail Pharmacy prescription fill data is readily accessible
  - The Pharmacy Industry already extensive users of Healthcare I/T
  - Retail Pharmacy accustomed to using and sharing for appropriate purposes
  - Capable of immediate impact for potential clinical implementations
- Full Clinical Data
  - Complete PHI, not de-identified data
  - All prescriptions, all patients, all sources, all payment types
  - Each dispensing along with pick up date & time

## Pharmacies want to participate

### **Pharmacies recognize value of expanding their role in providing Healthcare**

- **Balancing Goals and Realities:**
  - Increase interoperability with other Healthcare providers
  - Better serve their customers/patients and communities
  - Manage access to the data before someone else does
  - Don't significantly increase risk or liability
  - Don't provide advantage to potential competitors
  - Don't break the bank

## Top Clinical Demands

- **Requested Data Uses**

- Electronic Medical Records (EMR) systems Decision Support
- Adherence & Compliance Programs
- Hospital Medication Reconciliation Requirement
- Medication Therapy Management Programs
- Personal Health Record Solutions
- The Patient Centered Medical Home
- State & Federal Prescription Drug Monitoring & Management Programs

## Personal Health Records

### **Basic Concept:**

Make patients' health care information accessible and organized and they will make more informed decisions and better manage their own health care.

- Concept and solutions have been around a long time (in I/T terms).
- Potential for improving outcomes, lowering costs, educating patients on their therapy, enabling more personal responsibility, and more.
- Strong backing from Government, Healthcare, Patient Advocacy and other groups.
- The technology seems pretty straight forward.

*So, why doesn't everybody have one?*

- Healthcare Interoperability is bringing the concept back to the forefront

## Availability of PHR solutions

- PHRs are available from multiple sources with varying capabilities
  - Standalone Internet Website Solutions
  - Healthcare Provider Organizations
  - Employer Provided Vendor Solutions
  - Insurance Plan Companies
  - Retail Pharmacy Chains
  - Regional Health Information Exchanges
  - National Integrated Internet Offerings
  
- Each has its advantages and limitations
  
- Each must solve the basic challenges of accessing and managing PHI data

# Consumer Acceptance of PHRs

## Factors determining a consumer's selection and usage

- Who do they associate with managing their Healthcare?
- Who do they trust to have access to their private health information?
- Confidence in privacy and security
- Ease of obtaining, accessing, and managing their records
- Scope of function and services
- Incentives (discounts, coupons, payments, reward programs)
- Visible and tangible results due to usage
  
- Acceptance challenge: Some patients who would benefit most from sustained use of a PHR can be the least likely to be able to access, or, willing to invest their time.
- But the most motivated patients (or their caregivers) have found the tools invaluable in managing their sometimes complex and expensive healthcare requirements.

## Who pays the cost of PHRs?

**Basic Assumption:** All PHR providers have a strong patient advocacy and therapeutic outcomes improvement goal and motivation.

**Business models surrounding PHRs vary along with provider:**

- Advertising, referrals, click-through fees, affiliations
- Healthcare Organization patient outreach and retention
- Employer and Payer funding based on cost avoidance and reduction
- Customer service, competitive differentiation, revenue continuity
- Federal, state, and institutional grants and programs
- Brand awareness and expansion
- Infrastructure building for future opportunities

**Consistent Finding:** Patients do not want to pay out of pocket for a PHR.

**Sustainability:** Even some of the best PHR solutions and programs have found it difficult to financially justify PHRs for patients solely on adherence and compliance results.

## Where do PHRs get their data?

### Sources for PHR data population:

- Patient Self Entered
- Provider EMR and Healthcare Organization Systems
- Integrated Regional Exchange
- Internal Systems (Retail)
- Payer Claims Data
- Direct from Retail Pharmacy
- Data Aggregators

Key Point for Pharmacies – Whether you choose to provide data direct, at a regional level, or via an Aggregator, you will want to establish who owns your data and how it may be used even after it is out of your hands.

## Protecting data in a PHR environment

PHR solutions present a unique combination of data protection requirements

- Authentication
- Patient Consent
- Privacy Regulations (HIPAA, ARRA)
- Security
- Risk & Liability
- Sensitive Medication Restrictions

# Protecting data in a PHR environment

## Authentication

- How do you know the user is who he says he is?
  - Face to face credentialing is effective but an expensive logistical challenge
  - Existing patient relationship (address on file, US mail) may work for some
  - Online remote authentication is needed for most national, web based solutions
- Remote online authentication utilizes data accessible to the provider to ask questions only the authentic individual should be able to answer.
  - Banks have used this technique successfully using account balances, etc.
  - Healthcare organizations are starting to use based on their unique data.
  - Third party Authentication Services have demonstrated the ability to effectively do so based off of publicly accessible but highly specific data.

Authentication is a significant logistical and/or technological challenge to most PHR providers and an important service aspect to verify for any organization providing data.

## Protecting data in a PHR environment

### **Patient Consent**

- Patients should provide explicit consent:
  - For the data source (Pharmacy) to provide data to the PHR provider
  - For the PHR provider to display and disclose it via the PHR account
  - For the PHR provider to allow access by any third party, including doctors
- The data sources (Pharmacy) should require confirmation from the PHR that the patient's consent is on file allowing the source to send the data to the PHR.
  - Standard HIPAA Privacy Statement Disclosure may not be sufficient
  - Potential contractual requirement, or, other form of verification
- The Patient Consent should be explicit concerning Sensitive Medications
  - Rational arguments on both sides: Provide or Don't Provide.
  - Some states have specific laws or regulations to consider
  - PHR and data source should define policy and be explicit via Consent form

While highly important, Patient Consent can be handled in an efficient and reliable process at the time the patient signs up for a PHR.

# Protecting data in a PHR environment

## Privacy

- Patient Expectations
  - Not just a legal issue, but, also a Customer Satisfaction issue.
  - Patient disclosure and consent is the base
  - Policy and procedure for preventing disclosure by Patient and Prescription
- State & Federal Regulations
  - Sensitive Medication restrictions may differ by state or data source
- HIPAA
  - Pharmacy has grown accustomed to patient disclosure process
  - Some PHR providers have taken stand that they are not Business Associates
- ARRA
  - Raises the bar significantly above HIPAA
  - Specific language to make PHR type providers Business Associates
    - Some providers still challenging

# Protecting data in a PHR environment

## Security

- Obvious requirement and priority in today's Internet age
  - Highly sensitive, potentially valuable, tempting target
  
- Physical Protection of Data
  - During transfer or query process from pharmacy to PHR or Aggregator
  - During long term storage at PHR or Aggregator
  - Of individual Patient's PHR records storage (online, local, portable)
  
- Secured versus Unsecured Data
  - Important topic in new ARRA legislation
  - Determines level of action required upon data breach
  - Not just preventing access, but, if accessed is data useable
  - Encryption of data to national standard

## ARRA Legislation

- **American Recovery and Reinvestment Act of 2009 (“ARRA”)**
  - Signed February 17, 2009
  - \$790 billion allocated for economic stimulus
  - In the aggregate, approximately \$30 billion is allocated towards the improvement of healthcare:
    - Health IT
    - Training for more primary care physicians
    - Research on chronic diseases
    - Community health centers
    - “Comparative Effectiveness” research

## HITECH section of ARRA

- **Health Information Technology for Economic and Clinical Health Act**
  - Includes \$19 billion for Health IT
  - Includes new privacy and security provisions
- \$17 billion      **Physician Incentives**  
Incentive Bonuses from Medicare/Medicaid
- \$2 billion      **HHS Discretionary Funds (For Use By National Coordinator of Health IT)**  
Standards Development, Grants (AHRQ, HRSA, CMS), HIE Infrastructure, Loans to the States for EHR, Regional HIT Resource Centers, Telemedicine, Efficacy Studies

New Privacy and Security requirements apply to your pharmacy regardless of whether you get any of the ARRA/HITECH incentive payments.

## HITECH Privacy & Security

- HITECH expands privacy and security protections
- Are in addition to the HIPAA Statute and Privacy and Security Rules
- Changes and increases enforcement activities
- Applies provisions directly to entities not currently covered by HIPAA
  - Business Associates
  - Healthcare Information Exchanges (HIEs)
  - Regional HIEs
  - e-Prescribing Gateways
  - Personal Health Records (PHRs)

### Interim Final Rule on Breach Notification for Unsecured PHI

- Published August 24, 2009
- <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

## HITECH – Breach Notification

- Pre-HITECH, HIPAA does not require notification of breaches.
- Post-HITECH, a Covered Entity must notify affected individuals of breaches.
- Exceptions:
  - Where person who received it cannot reasonably have been able to retain it
  - Unintentional acquisition, access, or use within scope of employment or professional relationship, and information does not go any further
  - Inadvertent disclosure within facility, and information does not go any further
- Only breaches of unsecured information trigger notification requirement.
- Law defines notice requirements:
  - Content, Method, and Timing of notification to individual, HHS, media
- Clarifications in Interim Final Rule:
  - Defines encryption technologies needed for secure information.
  - Establishes risk & harm assessment to determine if breach requires notification.
  - Notification provisions preempt conflicting state laws, but not additional ones.
- Effective Date: September 23, 2009

## HITECH – HIPAA Extension

- Pre-HITECH in HIPAA
  - Business Associates were bound by contract only
  - Must use appropriate security safeguards and other requirements
  - Only enforcement was a breach of contract claim
  
- Now through HITECH
  - Business Associates are directly bound by certain provisions of HIPAA Security and Privacy Rules
  - HIPAA civil and criminal penalties are extended to Business Associates regarding security provisions and certain privacy provisions
  - Clarifies that HIEs, PHRs, e-Prescribing Gateways and other entities must have business associate agreements with Covered Entities

Even after this legislation, some national PHR providers are still evaluating their position on if they are Business Associates to the data providers

## HITECH – Restrictions on Disclosure

- Pre-HITECH, a Covered Entity was not required to comply with a request by a patient to limit appropriate PHI disclosure
- Post-HITECH, a Covered Entity must restrict disclosure of PHI to a health plan upon request by a patient if the service was paid for in cash
  - Potentially conflicts with today's workflow of processing the claim for a prescription prior to the patient reaching or contacting the pharmacy
  - Plans routinely request the data for waste, fraud, and abuse auditing
  - Such patients could be stuck in the Medicare Part D donut hole
- Effective Date: 1 year (February 17, 2010)

Interpretation and questions remain on how this provision can be implemented without significant impact to customer service and operational efficiency

## HITECH – Accounting for Disclosure

- Pre-HITECH, a Covered Entity (and by extension a Business Associate) does not have to account for disclosure if for payment, treatment, or operations
- Post-HITECH, a Covered Entity (and by extension a Business Associate) must make accounting of all disclosures over the previous three years upon patient request even if for payment, treatment, or operations
  - Would require tracking of all disclosures, appropriate or breach
  - Focus is on external disclosures, not internal organization use
  - Could be very costly for pharmacy organizations
- Effective Date:
  - Current users: January 1, 2014 (may extend to 2016)
  - New users: January 1, 2011 or start date (may extend to 2013)

## HITECH – Access to Records

- Under HITECH, Covered Entities using an EHR must provide an electronic copy of patient PHI if requested by the individual
  - Does this apply to a pharmacy?
  - Definition of “using an EHR” is not clear in this regard.
  
- Response must be provided to the patient in electronic form
  - Questions remain on what satisfies an “electronic form”
  - Fax? Via website? To a PHR?
  
- Any fee charged would be limited to labor cost to respond
  - Calculation of any fee is not yet further defined
  
- Effective Date: 1 year (February 17, 2010)

## HITECH – Prohibition on sales of PHI

- No remuneration can be paid for the exchange of PHI, subject to certain exceptions
- The exceptions include:
  - Public Health
  - Treatment of the individual
  - Research
  - Providing a copy of the record to a patient
- Is providing data to a PHR covered under the “copy to patient” exception?
  - Would affect if a pharmacy can receive payment for the data
- Effective Date: TBD
  - 18 months for Regulations plus 6 months

## HITECH – Marketing & Minimum Necessary

- Authorization for marketing
  - Patient authorization required for marketing if the Covered Entity is receiving remuneration from outside entity for communication to a patient
  - Communications for currently prescribed drugs do not require patient authorization though subject to a “reasonable” payment limit
  - Effective Date:
    - One year (February 17, 2010)
  
- Definition of minimum necessary
  - HHS Secretary to issue guidance (not regulations) on what constitutes “minimum necessary” under HIPAA within 18 months from enactment
  - Regulations:
    - Guidance to be issued in 18 months
  - Effective Date:
    - Guidance goes into effect one year after issuance of guidance

## HITECH – Additional PHR related items

- Breach notification provisions apply to PHRs
  - PHRs must comply with breach notification provisions
  - FTC will enforce these provisions
  - Regulations:
    - FTC required to issue within 180 days
  - Effective Date:
    - 30 days after rule publication
  
- HHS (& FTC) to conduct study on privacy and security requirements for PHR vendors and applications
  - Due by February 17, 2010

## HITECH – Increased enforcement

- Direct accountability for Business Associates
- Criminal penalties apply against individuals
  - Including employees of Covered Entities
- HHS Secretary must impose civil monetary penalties for noncompliance due to willful neglect
- HHS Secretary must formally investigate any complaint if preliminary investigation indicated a possible violation
- State Attorney Generals have right to enforce

## Where are PHRs heading?

### The Patient Centered Medical Home

- A healthcare environment of uninterrupted care managed between a personal provider and an engaged patient, utilizing and integrating core HIT tools
  - Ongoing relationship with a personal physician
  - Physician directed medical care based on clinical best practices
  - Coordinated care and information between a patient's providers
  - Improved medication therapy management through counseling and programs
  - IT tool utilization to improve quality, safety, and efficiency

“I support the concept of a patient-centered medical home, and as part of my health care plan, I will encourage and provide appropriate payment for providers who implement the medical home model, including physician-directed, interdisciplinary teams, care management and care coordination programs, quality assurance mechanisms, and health IT systems which collectively will help to improve care.”

- President Obama

## The Patient Centered Medical Home

- Ability of providers, patients and other members of a person's health team to communicate among themselves and in the process of care delivery
  - Potential for patient to know or control which caregivers have access
- Ability of patients to be informed and literate about their health and medical conditions and appropriately self-manage with monitoring and coaching from providers
  - Medications, labs, condition and therapy records accessible and organized

The synthesis of PHR, EMR, MTM and HIE capabilities into an integrated approach of healthcare for the whole patient

## Participating in PHRs and other Clinical uses

- Determine your patient and business drivers, and, their business impact
  - Customer services on par with top competitors
  - Leadership in Healthcare for the markets you serve
  - Patient adherence, compliance, persistency....and with your pharmacy
  
- Review, understand, and apply ARRA, state, and other regulatory requirements to your procedures and decisions regarding data sharing
  
- Work direct with PHR provider or via third party aggregator?
  - Considerations:
    - Staff expertise on related issues (patient consent, authentication, ...)
    - One PHR or potential for multiple clinical data uses in future
    - Resources for establishing contracts, policies, data feeds, etc
    - Who is responsible for authenticating patients/users of the PHR?
    - Cost efficiency

## Wrap up

- Pharmacy clinical data continues to gain importance in Healthcare
- Initiatives involving PHRs, Patient Centered Medical Home, and other appropriate solutions continue to expand in scope and availability
- There is significant value to the pharmacy and the pharmacy industry to increase integration into local and/or national HIT initiatives
- Significant new legislation affects the access and use of pharmacy data
- Resources are available to pharmacies interested in participating but who don't want to do so on their own

# Questions?

Thank You

Rusty Keith

*[rusty.keith@surescripts.com](mailto:rusty.keith@surescripts.com)*