



## Privacy & Security Considerations for Health Services Research

---

Deven McGraw, JD, MPH  
Linda Dimitropoulos, PhD  
Jeff Loughlin, MHA

December 15, 2011

### **Privacy & Security Considerations for Health Services Research**

Deven McGraw, JD, MPH  
Linda Dimitropoulos, PhD  
Jeff Loughlin, MHA  
December 15, 2011



## Agenda

- Welcome
  - Barbara Lund, TA Team, Massachusetts eHealth Collaborative
  - Angela Lavanderos, AHRQ, Program Analyst
- Grantee Introductions
- Speaker Presentations
  - Deven McGraw
  - Linda Dimitropoulos
  - Jeff Loughlin
- Questions & Discussion

### Agenda

- Welcome
  - Barbara Lund, TA Team, Massachusetts eHealth Collaborative
  - Angela Lavanderos, AHRQ, Program Analyst
- Grantee Introductions
- Speaker Presentations
  - Deven McGraw
  - Linda Dimitropoulos
  - Jeff Loughlin
- Questions & Discussion



## Technical Assistance Overview

- Goal: To support grantees in the meaningful progress and on-time completion of Health IT Portfolio-funded grant projects
- Technical Assistance (TA) is delivered in three ways:
  - One-on-one individual TA
  - Multi-grantee webinars
  - Multi-grantee peer-to-peer teleconferences
- Ongoing evaluation to improve TA offerings

### Technical Assistance Overview

- Goal: To support grantees in the meaningful progress and on-time completion of Health IT Portfolio-funded grant projects
- Technical Assistance (TA) is delivered in three ways:
  - One-on-one individual TA
  - Multi-grantee webinars
  - Multi-grantee peer-to-peer teleconferences
- Ongoing evaluation to improve TA offerings



## Key Resources

- AHRQ National Resource Center for Health IT
  - [www.healthit.ahrq.gov](http://www.healthit.ahrq.gov)
- AHRQ Points of Contact
  - Vera Rosenthal, [vera.rosenthal@ahrq.hhs.gov](mailto:vera.rosenthal@ahrq.hhs.gov)
- AHRQ NRC TA Team
  - Kai Carter and Allyson Miller: Booz Allen Hamilton; [carter\\_nzinga@bah.com](mailto:carter_nzinga@bah.com); [miller\\_allyson@bah.com](mailto:miller_allyson@bah.com)
  - Barbara Lund and Rachel Kell: Massachusetts eHealth Collaborative, [NRC-TechAssist@AHRQ.hhs.gov](mailto:NRC-TechAssist@AHRQ.hhs.gov)

### Key Resources

- AHRQ National Resource Center for Health IT
  - [www.healthit.ahrq.gov](http://www.healthit.ahrq.gov)
- AHRQ Points of Contact
  - Vera Rosenthal, [vera.rosenthal@ahrq.hhs.gov](mailto:vera.rosenthal@ahrq.hhs.gov)
- AHRQ NRC TA Team
  - Kai Carter and Allyson Miller: Booz Allen Hamilton; [carter\\_nzinga@bah.com](mailto:carter_nzinga@bah.com); [miller\\_allyson@bah.com](mailto:miller_allyson@bah.com)
  - Barbara Lund and Rachel Kell: Massachusetts eHealth Collaborative, [NRC-TechAssist@AHRQ.hhs.gov](mailto:NRC-TechAssist@AHRQ.hhs.gov)



## Housekeeping

- All phone lines are UN-muted
- You may mute your own line at any time by pressing \*6 (or via your phone's mute button); press \* 7 to un-mute
- Questions may also be submitted at any time via 'Chat' feature on webinar console
- Online survey for completion by all participants at conclusion of Webinar
- Discussion summary will be distributed to attendees

### Housekeeping

- All phone lines are UN-muted
- You may mute your own line at any time by pressing \*6 (or via your phone's mute button); press \* 7 to un-mute
- Questions may also be submitted at any time via 'Chat' feature on webinar console
- Online survey for completion by all participants at conclusion of Webinar
- Discussion summary will be distributed to attendees



## Today's Presentation

---

### Privacy & Security Considerations for Health Services Research

Facilitator: Barbara Lund, AHRQ NRC TA Team,  
Massachusetts eHealth Collaborative

#### **Today's Presentation**

#### **Privacy & Security Considerations for Health Services Research**

Facilitator: Barbara Lund, AHRQ NRC TA Team, Massachusetts eHealth  
Collaborative



## Today's Objectives

- Provide an overview of the privacy and security issues of importance to health care IT researchers
- Outline approaches for researchers to ensure the security of patient data through appropriate policies and procedures governing their team's use of and access to PHI
- Discuss technical considerations for data use and exchange, particularly as relates to EHRs and HIE
- Share experiences and recommendations amongst grantees

### Today's Objectives

- Provide an overview of the privacy and security issues of importance to health care IT researchers
- Outline approaches for researchers to ensure the security of patient data through appropriate policies and procedures governing their team's use of and access to PHI
- Discuss technical considerations for data use and exchange, particularly as relates to EHRs and HIE
- Share experiences and recommendations amongst grantees



## Grantee Roll Call

---

- Name, Organization, Project PI

### **Grantee Roll Call**

- Name, Organization, Project PI



## Today's Presenters

- **Deven McGraw, JD, MPH** - Director of the Health Privacy Project at the Center for Democracy and Technology
  - Policies Governing Uses/Disclosures of Health Information for Research
- **Linda Dimitropoulos, PhD** - Director for the Center for the Advancement of HIT at RTI International
  - Privacy and Security Requirements Governing Research with Clinical Data: Some Considerations for Health Services Researchers
- **Jeff Loughlin, MHA** - Executive Director of the Regional Extension Center of NH
  - Protecting Patient Data: Privacy and Security of Electronic Health Records (EHR)

### Today's Presenters

- Deven McGraw, JD, MPH - Director of the Health Privacy Project at the Center for Democracy and Technology
  - Policies Governing Uses/Disclosures of Health Information for Research
- Linda Dimitropoulos, PhD - Director for the Center for the Advancement of HIT at RTI International
  - Privacy and Security Requirements Governing Research with Clinical Data: Some Considerations for Health Services Researchers
- Jeff Loughlin, MHA - Executive Director of the Regional Extension Center of NH
  - Protecting Patient Data: Privacy and Security of Electronic Health Records (EHR)



**Deven McGraw**

---

## **Policies Governing Uses/Disclosures of Health Information for Research**

**Deven McGraw**

**Policies Governing Uses/Disclosures of Health Information for Research**



## HIPAA Basics

- Governs covered entities (most health care providers) and contractors acting on their behalf (business associates)
  - BAs conducting research for covered entities must execute business associate agreement
  - HIEs are business associates
- Privacy rule sets permitted uses and disclosures of protected (identifiable) health information (PHI)
- Security rule sets forth required and addressable protections for electronic PHI.

### HIPAA Basics

- Governs covered entities (most health care providers) and contractors acting on their behalf (business associates)
  - BAs conducting research for covered entities must execute business associate agreement
  - HIEs are business associates
- Privacy rule sets permitted uses and disclosures of protected (identifiable) health information (PHI)
- Security rule sets forth required and addressable protections for electronic PHI.



## HIPAA Basics (cont.)

- Quality assessment & improvement activities are part of “health care operations” – consent not required for use and disclosure of PHI for these purposes
  - But not “operations” if primary purpose is to contribute to “generalizable” knowledge
- Research is systematic investigation designed to develop or contribute to generalizable knowledge
- If research, specific authorization of patient required – with exceptions

### HIPAA Basics (cont.)

- Quality assessment & improvement activities are part of “health care operations” – consent not required for use and disclosure of PHI for these purposes
  - But not “operations” if primary purpose is to contribute to “generalizable” knowledge
- Research is systematic investigation designed to develop or contribute to generalizable knowledge
- If research, specific authorization of patient required – with exceptions



## Federal Common Rule

- Governs most federally funded health care research
- Same definition of research as in HIPAA
- Like HIPAA, requires informed consent for research using identifiable information – but IRB can waive using similar criteria
- Also, IRB approval required if research using clinical data – but can be done on expedited basis

### Federal Common Rule

- Governs most federally funded health care research
- Same definition of research as in HIPAA
- Like HIPAA, requires informed consent for research using identifiable information – but IRB can waive using similar criteria
- Also, IRB approval required if research using clinical data – but can be done on expedited basis



## Less Identifiable = Less Risk = Fewer Restrictions

- Limited data set (LDS) - removal of certain categories of identifiers
- De-identified data – removal of more categories of identifiers
  - not PHI; largely not regulated by HIPAA (can use for any purpose)

### **Less Identifiable = Less Risk = Fewer Restrictions**

- Limited data set (LDS) - removal of certain categories of identifiers
- De-identified data – removal of more categories of identifiers
  - not PHI; largely not regulated by HIPAA (can use for any purpose)



## Other Applicable Laws/Policies

- State medical privacy laws may apply
- HIEs may have specific policies that apply
- Federal or state grant funding conditions
- Genetic Nondiscrimination Act
- Federal Substance Abuse Confidentiality Regulations

### **Other Applicable Laws/Policies**

- State medical privacy laws may apply
- HIEs may have specific policies that apply
- Federal or state grant funding conditions
- Genetic Nondiscrimination Act
- Federal Substance Abuse Confidentiality Regulations



## Developments to Watch

- Governance rule for “Nationwide Health Information Network”
  - Expected early 2012
  - To be issued by ONC
  - Likely to govern HIEs access, use and disclosure of identifiable information
  - May cover other ONC/CMS grantees
  - May incorporate Health IT Policy Committee recommendations on fair information practices and consent

### Developments to Watch

#### Governance rule for “Nationwide Health Information Network”

- Expected early 2012
- To be issued by ONC
- Likely to govern HIEs access, use and disclosure of identifiable information
- May cover other ONC/CMS grantees
- May incorporate Health IT Policy Committee recommendations on fair information practices and consent



## Developments to Watch (cont.)

- **ONC QueryHealth Initiative**
  - Expected to develop standards for distributed networks for population health research (2012)
- **Potential Changes to Common Rule (ANPRM comment period closed Oct. 2011)**
- **Finalization of HITECH changes to HIPAA Privacy Rule (accounting of disclosure rule changes probably not finalized until later 2012)**
- **Proposed rule for stage 2 Meaningful Use; beginning discussions for Stage 3**

### **Developments to Watch (cont.)**

- **ONC QueryHealth Initiative**
  - Expected to develop standards for distributed networks for population health research (2012)
- **Potential Changes to Common Rule (ANPRM comment period closed Oct. 2011)**
- **Finalization of HITECH changes to HIPAA Privacy Rule (accounting of disclosure rule changes probably not finalized until later 2012)**
- **Proposed rule for stage 2 Meaningful Use; beginning discussions for Stage 3**

**Questions?**

**Questions?**



**Linda Dimitropoulos**

---

**Privacy and Security Requirements  
Governing Research with Clinical  
Data: Some Considerations for Health  
Services Researchers**

**Linda Dimitropoulos**

**Privacy and Security Requirements Governing Research with Clinical Data:  
Some Considerations for Health Services Researchers**



## The Promise of Clinical Data for Research

- Access to electronic clinical information is critical to advancing health services research and medical knowledge to support the learning health system
- Balancing the needs of researchers for access to data, the needs of patients for privacy, and navigating the regulations continues to be a challenge

### **The Promise of Clinical Data for Research**

- Access to electronic clinical information is critical to advancing health services research and medical knowledge to support the learning health system
- Balancing the needs of researchers for access to data, the needs of patients for privacy, and navigating the regulations continues to be a challenge



## Regulations and Guidance: Privacy and Security Laws

- The Privacy Act of 1974
- HIPAA Privacy and Security Rules
- International Privacy Laws
  - E.g., The European Union Directive
- Confidential Information Protection & Statistical Efficiency Act of 2002 (CIPSEA)
- Federal Information Security Management Act of 2003 (FISMA)
  - Set by NIST, follows the Federal Information Processing Standards (FIPS) used to set data security levels

### **Regulations and Guidance: Privacy and Security Laws**

- The Privacy Act of 1974
- HIPAA Privacy and Security Rules
- International Privacy Laws
  - E.g., The European Union Directive
- Confidential Information Protection & Statistical Efficiency Act of 2002 (CIPSEA)
- Federal Information Security Management Act of 2003 (FISMA)
  - Set by NIST, follows the Federal Information Processing Standards (FIPS) used to set data security levels



## What types of projects generally require higher levels of data protection?

- Any project that is designated as FIPS moderate security level by the funding agency
- Any which involve data files with SSNs (e.g., CMS data analysis projects)
- Any with direct identifiers and very sensitive information
- Any projects that require a Business Associate Agreement
- Any projects that involve classified information

### **What types of projects generally require higher levels of data protection?**

- Any project that is designated as FIPS moderate security level by the funding agency
- Any which involve data files with SSNs (e.g., CMS data analysis projects)
- Any with direct identifiers and very sensitive information
- Any projects that require a Business Associate Agreement
- Any projects that involve classified information



## What is "PII"?

- **Personally identifiable information (PII):**  
Information that can be used to uniquely identify a single individual - or can be used with other sources to uniquely identify a single individual - such as:
  - Full Name
  - Address
  - Telephone number
  - E-mail address
  - Social Security Number
  - Other identifying numbers (drivers license number, credit card numbers, medical records number)
  - Biometric records

### What is "PII"?

Personally identifiable information (PII): Information that can be used to uniquely identify a single individual - or can be used with other sources to uniquely identify a single individual - such as:

- Full Name
- Address
- Telephone number
- E-mail address
- Social Security Number
- Other identifying numbers (drivers license number, credit card numbers, medical records number)
- Biometric records



## What is PHI?

- **Protected Health Information (PHI):**
  - Personally identifiable information that relates to a person's health, medical treatment or payment, and which was obtained from a "covered entity" (health care provider, health plan, or healthcare clearinghouse), as defined by HIPAA.
- HIPAA defines 18 identifiers that constitute PHI - these include direct identifiers (as for PII) as well as dates and geographic indicators
- PHI is NOT the same thing as PII—PHI only applies to projects that are covered by HIPAA.

### What is PHI?

- Protected Health Information (PHI):
  - Personally identifiable information that relates to a person's health, medical treatment or payment, and which was obtained from a "covered entity" (health care provider, health plan, or healthcare clearinghouse), as defined by HIPAA.
- HIPAA defines 18 identifiers that constitute PHI - these include direct identifiers (as for PII) as well as dates and geographic indicators
- PHI is NOT the same thing as PII—PHI only applies to projects that are covered by HIPAA.



## Types of Research Affected by HIPAA

- 1. Research that uses existing PHI:
  - Health services research
  - Medical records abstraction
  - Use of databases or registries
- 2. Research that includes treatment of research participants (may generate new PHI):
  - Clinical trials

### **Types of Research Affected by HIPAA**

#### 1. Research that uses existing PHI:

- Health services research
- Medical records abstraction
- Use of databases or registries

#### 2. Research that includes treatment of research participants (may generate new PHI):

- Clinical trials



## De-identification

- Under HIPAA, health information that is de-identified is not PHI so is not covered under the Privacy Rule.
- Two acceptable de-identification methods:
  - Safe Harbor - remove 18 specified data elements from the data set
  - Statistical Verification - statistician states that there is “very small risk” of re-identification
  - The covered entity must have no actual knowledge that an individual could be re-identified.

### De-identification

- Under HIPAA, health information that is de-identified is not PHI so is not covered under the Privacy Rule.
- Two acceptable de-identification methods:
  - Safe Harbor - remove 18 specified data elements from the data set
  - Statistical Verification - statistician states that there is “very small risk” of re-identification
  - The covered entity must have no actual knowledge that an individual could be re-identified.



## Research Use and Disclosure with Patient Authorization

- Authorization form must include several elements:
  - What information is to be used/disclosed
  - Who may use/disclose the information
  - Who will receive information
  - Purpose of use/disclosure
  - Right to revoke authorization
  - Treatment not affected by granting authorization
  - Expiration date of authorization (can be indefinite)
  - Patient's signature and date

### **Research Use and Disclosure with Patient Authorization**

Authorization form must include several elements:

- What information is to be used/disclosed
- Who may use/disclose the information
- Who will receive information
- Purpose of use/disclosure
- Right to revoke authorization
- Treatment not affected by granting authorization
- Expiration date of authorization (can be indefinite)
- Patient's signature and date



## Research Use and Disclosure of PHI without Patient Authorization

- There are four options available under HIPAA:
  - OPTION 1: Get an IRB or Privacy Board waiver
  - OPTION 2: Provide documentation that PHI will be used only for activities “preparatory to research”
  - OPTION 3: Provide documentation that the research will involve only decedent’s PHI
  - OPTION 4: Use only a “limited data set” for research, public health, or health care operations

### Research Use and Disclosure of PHI without Patient Authorization

There are four options available under HIPAA:

- OPTION 1: Get an IRB or Privacy Board waiver
- OPTION 2: Provide documentation that PHI will be used only for activities “preparatory to research”
- OPTION 3: Provide documentation that the research will involve only decedent’s PHI
- OPTION 4: Use only a “limited data set” for research, public health, or health care operations



## Limited Data Sets and DUAs

- A limited data set may include the following data elements (this differs from de-identified data):
  - Person’s initials (but not full name)
  - Complete dates
  - City, town, State, 5-digit Zip code
  - Link code (i.e., study ID for re-identification by the covered entity)
  - Any other item that is not specifically listed in the list of exclusions

### Limited Data Sets and DUAs

A limited data set may include the following data elements (this differs from de-identified data):

- Person’s initials (but not full name)
- Complete dates
- City, town, State, 5-digit Zip code
- Link code (i.e., study ID for re-identification by the covered entity)
- Any other item that is not specifically listed in the list of exclusions



## DUA required for a covered entity to release a Limited Data Set

- A Data Use Agreement establishes:
  - The permitted uses/disclosures of the data set by the recipient
  - Who is permitted to use or receive the data set

### **DUA required for a covered entity to release a Limited Data Set**

A Data Use Agreement establishes:

- The permitted uses/disclosures of the data set by the recipient
- Who is permitted to use or receive the data set



## DUAs (cont.)

- The agreement must also provide that the recipient will:
  - Not use or further disclose the information outside the purposes stated in the agreement
  - Use safeguards to protect the data
  - Report any use/disclosures outside the agreement to the covered entity
  - Ensure that others to whom it releases data set abide by same conditions
  - Not identify or contact the individuals

### DUAs (cont.)

The agreement must also provide that the recipient will:

- Not use or further disclose the information outside the purposes stated in the agreement
- Use safeguards to protect the data
- Report any use/disclosures outside the agreement to the covered entity
- Ensure that others to whom it releases data set abide by same conditions
- Not identify or contact the individuals



## Roles of the IRB (or Privacy Board)

- At RTI, the IRB (rather than a Privacy Board) oversees all research compliance issues and specifically for health services research, HIPAA compliance:
  - Grant requests for Waivers of Authorization
  - Review Authorization forms (or consent language) for HIPAA elements
  - Review plans to use de-identified data
  - Assure that Data Use Agreements are in place if Limited Data Set is used
  - Review “preparatory to research” plans
  - Review data security plans

### **Roles of the IRB (or Privacy Board)**

At RTI, the IRB (rather than a Privacy Board) oversees all research compliance issues and specifically for health services research, HIPAA compliance:

- Grant requests for Waivers of Authorization
- Review Authorization forms (or consent language) for HIPAA elements
- Review plans to use de-identified data
- Assure that Data Use Agreements are in place if Limited Data Set is used
- Review “preparatory to research” plans
- Review data security plans



## Other Considerations for Health Services Researchers

- Non-research HIPAA requirements will also affect the covered entities with whom you work
- Some covered entities will require you to use their IRB or Privacy Board
- May incorporate authorization language into consent, or use separate authorization form
- State-level privacy laws may be more stringent than HIPAA
- Be prepared for audits and compliance

### Other Considerations for Health Services Researchers

- Non-research HIPAA requirements will also affect the covered entities with whom you work
- Some covered entities will require you to use their IRB or Privacy Board
- May incorporate authorization language into consent, or use separate authorization form
- State-level privacy laws may be more stringent than HIPAA
- Be prepared for audits and compliance



---

**Questions?**

**Questions?**



**Jeff Loughlin**

---

Protecting Patient Data:  
Privacy and Security of Electronic Health  
Records (EHR)

**Jeff Loughlin**

**Protecting Patient Data:**

**Privacy and Security of Electronic Health Records (EHR)**



## Structured Data Needs

- American Recovery and Reinvestment Act (ARRA)
  - Health Information Technology for Economic and Clinical Health (HITECH) – Meaningful Use
- Payment Reform
  - Patient Centered Medical Home (PCMH)
  - Accountable Care Organizations (ACO)
- National Quality Strategy
  - Quality Improvement Initiatives
  - Million Hearts Campaign

### Structured Data Needs

- American Recovery and Reinvestment Act (ARRA)
  - Health Information Technology for Economic and Clinical Health (HITECH)
    - Meaningful Use
- Payment Reform
  - Patient Centered Medical Home (PCMH)
  - Accountable Care Organizations (ACO)
- National Quality Strategy
  - Quality Improvement Initiatives
  - Million Hearts Campaign



## HITECH – Meaningful Use

- Use of certified EHR in a meaningful manner (e.g., e-prescribing)
- Use of certified EHR technology for electronic exchange of health information to improve quality of health care
- Use of certified EHR technology to submit clinical quality measures (CQM) and other such measures selected by the Secretary

### HITECH – Meaningful Use

- Use of certified EHR in a meaningful manner (e.g., e-prescribing)
- Use of certified EHR technology for electronic exchange of health information to improve quality of health care
- Use of certified EHR technology to submit clinical quality measures (CQM) and other such measures selected by the Secretary



## Data Requirements

- Patient Demographics
  - Includes Race and Ethnicity
- Problem List (ICD / SNOMED), Active Medications (Structured), Use of ePrescribing, Medication Allergies
- Lab Results (LOINC), Procedures (CPT), Test Results
- Vital signs (HT, WT, BP, BMI), Smoking Status

### Data Requirements

- Patient Demographics
  - Includes Race and Ethnicity
- Problem List (ICD / SNOMED), Active Medications (Structured), Use of ePrescribing, Medication Allergies
- Lab Results (LOINC), Procedures (CPT), Test Results
- Vital signs (HT, WT, BP, BMI), Smoking Status



## Data Exchange and Reporting

- Continuity of Care Document (C32-CCD)
  - Capability to Exchange CCD
- Submit Clinical Quality Measures (CQM)
  - National Quality Forum (NQF)
  - Physician Quality Reporting System (PQRS)
- Public Health Reporting
  - Immunization Registry
  - Syndromic Surveillance Data

### Data Exchange and Reporting

- Continuity of Care Document (C32-CCD)
  - Capability to Exchange CCD
- Submit Clinical Quality Measures (CQM)
  - National Quality Forum (NQF)
  - Physician Quality Reporting System (PQRS)
- Public Health Reporting
  - Immunization Registry
  - Syndromic Surveillance Data



## Privacy and Security

- **Objective:** Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities
- **Requirement:** Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process
  - 135(+/-) Identified Risk Areas
  - Addressable or Required by Policy or Procedure
  - Annual Review or Update with System Changes
  - Includes Business Associates

### Privacy and Security

- Objective: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities
- Requirement: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process
  - 135(+/-) Identified Risk Areas
  - Addressable or Required by Policy or Procedure
  - Annual Review or Update with System Changes
  - Includes Business Associates



## Policies and Procedures

- Protect Patient Health Information (PHI) – HIPAA
  - Patient Consent for Release of Information
- Physical Security of Hardware and Devices
  - Mobile Devices and Remote Access
- Password Management and Role-based Access
- Network Security and Data Encryption
- Data Back-up and Disaster Recovery Process

### **Policies and Procedures**

- Protect Patient Health Information (PHI) – HIPAA
  - Patient Consent for Release of Information
- Physical Security of Hardware and Devices
  - Mobile Devices and Remote Access
- Password Management and Role-based Access
- Network Security and Data Encryption
- Data Back-up and Disaster Recovery Process



## Health Information Exchange

- **Objective:** Capability to exchange key clinical information (CCD) among providers of care and patient authorized entities electronically
- **CMS FAQ:** Providers “may use any means of electronic transmission according to any transport standard(s)”
  - Encrypted WinZip and Simple Mail Transfer Protocol (SMTP)
  - Secure File Transfer Protocol (FTP)
  - Secure Socket Layer (SSL) Web Interface
  - Simple Object Access Protocol (SOAP), Representational State Transfer (REST)

### Health Information Exchange

- Objective: Capability to exchange key clinical information (CCD) among providers of care and patient authorized entities electronically
- CMS FAQ: Providers “may use any means of electronic transmission according to any transport standard(s)”
  - Encrypted WinZip and Simple Mail Transfer Protocol (SMTP)
  - Secure File Transfer Protocol (FTP)
  - Secure Socket Layer (SSL) Web Interface
  - Simple Object Access Protocol (SOAP), Representational State Transfer (REST)



## Patient Data Availability

- **Objective:** Provide patients with an electronic copy of their health information (CD / USB)
- **Objective:** Provide clinical summaries for patients for each office visit (Paper or Electronic)
- **Objective (Menu):** Provide patients with timely electronic access to their health information (Patient Portal)
- Reporting Requirements (CMS, Public Health)

### Patient Data Availability

- Objective: Provide patients with an electronic copy of their health information (CD / USB)
- Objective: Provide clinical summaries for patients for each office visit (Paper or Electronic)
- Objective (Menu): Provide patients with timely electronic access to their health information (Patient Portal)
- Reporting Requirements (CMS, Public Health)



## Practice Concerns

- Breach Notification and HIPAA Requirements
  - Patient / Public Disclosure Requirements
- Patient Consent for Health Information Exchange (HIE)
  - Centralized Data Repositories
  - State Privacy Laws
- PHI Access Audit Capability and Requirements
- Increased Focus on Technical Safeguards

### Practice Concerns

- Breach Notification and HIPAA Requirements
  - Patient / Public Disclosure Requirements
- Patient Consent for Health Information Exchange (HIE)
  - Centralized Data Repositories
  - State Privacy Laws
- PHI Access Audit Capability and Requirements
- Increased Focus on Technical Safeguards



## Discussion

---

- We welcome your comments and questions
- Reminder: press \*6 to mute; press \* 7 to un-mute
- Questions may also be submitted via 'Chat' feature on webinar console at any time

### **Discussion**

- We welcome your comments and questions
- Reminder: press \*6 to mute; press \* 7 to un-mute
- Questions may also be submitted via 'Chat' feature on webinar console at any time



## Final Comments

- Discussion Summary
  - Will be distributed to all Webinar participants and posted on the AHRQ TA website
- Evaluation Form
  - Online evaluation form will appear on your screen at conclusion of webinar; we value your input.
  - Thank you for joining us today!

### Final Comments

- Discussion Summary
  - Will be distributed to all Webinar participants and posted on the AHRQ TA website
- Evaluation Form
  - Online evaluation form will appear on your screen at conclusion of webinar; we value your input.
  - Thank you for joining us today!



## Panelist Bios

### Deven McGraw, JD, MPH

Deven McGraw is the Director of the Health Privacy Project at the Center for Democracy & Technology (CDT), where she promotes policies that protect individual privacy as personal health information is shared electronically. Ms. McGraw serves on the Health Information Technology (HIT) Policy Committee and chairs its Privacy and Security Workgroup (called the “Tiger Team”). She is a magna cum laude graduate of the Georgetown University Law Center and received her Master of Public Health from Johns Hopkins University.

Contact email: [deven@cdt.org](mailto:deven@cdt.org)

### Panelist Bios

#### Deven McGraw, JD, MPH

Deven McGraw is the Director of the Health Privacy Project at the Center for Democracy & Technology (CDT), where she promotes policies that protect individual privacy as personal health information is shared electronically. Ms. McGraw serves on the Health Information Technology (HIT) Policy Committee and chairs its Privacy and Security Workgroup (called the “Tiger Team”). She is a magna cum laude graduate of the Georgetown University Law Center and received her Master of Public Health from Johns Hopkins University.

Contact email: [deven@cdt.org](mailto:deven@cdt.org)



## Panelist Bios

### Linda Dimitropoulos, PhD

Dr. Linda Dimitropoulos is the director of the Center for the Advancement of Health Information Technology (CAHIT) at RTI International. The Center brings together a multidisciplinary group of clinical informaticians, policy analysts, researchers, and clinicians focused on improving health care delivery through the effective use of health IT. Dr. Dimitropoulos is a social psychologist with expertise in attitude change, measurement, and persuasive communications with applications to consumer behavior and decision making. She has 18 years of experience designing and managing health services research studies and currently leads several key federal contracts, including the Agency for Healthcare Research and Quality (AHRQ) Technical Assistance to Implement Health IT and HIE in Medicaid and CHIP contract. She serves as the program director for the National Resource Center for Health IT contracts also funded by AHRQ. Dr. Dimitropoulos led the Privacy and Security Solutions for Interoperable Health Information Exchange and the Health Information Security and Privacy Collaboration (HISPC) contracts for AHRQ and ONC, which studied the variation in federal and state health information privacy laws and policies governing electronic health information exchange.

Contact email: [lld@rti.org](mailto:lld@rti.org)

### Panelist Bios

#### Linda Dimitropoulos, PhD

Dr. Linda Dimitropoulos is the director of the Center for the Advancement of Health Information Technology (CAHIT) at RTI International. The Center brings together a multidisciplinary group of clinical informaticians, policy analysts, researchers, and clinicians focused on improving health care delivery through the effective use of health IT. Dr. Dimitropoulos is a social psychologist with expertise in attitude change, measurement, and persuasive communications with applications to consumer behavior and decision making. She has 18 years of experience designing and managing health services research studies and currently leads several key federal contracts, including the Agency for Healthcare Research and Quality (AHRQ) Technical Assistance to Implement Health IT and HIE in Medicaid and CHIP contract. She serves as the program director for the National Resource Center for Health IT contracts also funded by AHRQ. Dr. Dimitropoulos led the Privacy and Security Solutions for Interoperable Health Information Exchange and the Health Information Security and Privacy Collaboration (HISPC) contracts for AHRQ and ONC, which studied the variation in federal and state health information privacy laws and policies governing electronic health information exchange.

Contact email: [lld@rti.org](mailto:lld@rti.org)



## Panelist Bios

### Jeff Loughlin, MHA

Jeff is a Project Director with the Massachusetts eHealth Collaborative (MAeHC) and currently serves as the Director for the Regional Extension Center of New Hampshire, working with providers, practice leaders, medical and administrative staffs to ensure successful adoption and Meaningful Use of EHR technology in the medical office environment. Jeff has worked with the Collaborative for 6 years, providing a variety of consulting services to practice, and community based EHR and HIE initiatives. Prior to joining MAeHC, Jeff served as an information technology consultant at Boston Medical Center providing EHR implementation and training services for the outpatient medical departments. Before moving to the IT team, Jeff spent several years as a Practice Manager in a variety of outpatient settings at Boston Medical Center, Harvard Vanguard Medical Associates, and Boston City Hospital. Jeff is a US Army veteran with over 23 years of military service and is currently serving with the Massachusetts Army National Guard as a Medical Service Corps Lieutenant Colonel. Jeff holds a Master's Degree in Healthcare Administration from Simmons College in Boston.

Contact email: [jloughlin@maehc.org](mailto:jloughlin@maehc.org)

## Panelist Bios

### Jeff Loughlin, MHA

Jeff is a Project Director with the Massachusetts eHealth Collaborative (MAeHC) and currently serves as the Director for the Regional Extension Center of New Hampshire, working with providers, practice leaders, medical and administrative staffs to ensure successful adoption and Meaningful Use of EHR technology in the medical office environment. Jeff has worked with the Collaborative for 6 years, providing a variety of consulting services to practice, and community based EHR and HIE initiatives. Prior to joining MAeHC, Jeff served as an information technology consultant at Boston Medical Center providing EHR implementation and training services for the outpatient medical departments. Before moving to the IT team, Jeff spent several years as a Practice Manager in a variety of outpatient settings at Boston Medical Center, Harvard Vanguard Medical Associates, and Boston City Hospital. Jeff is a US Army veteran with over 23 years of military service and is currently serving with the Massachusetts Army National Guard as a Medical Service Corps Lieutenant Colonel. Jeff holds a Master's Degree in Healthcare Administration from Simmons College in Boston.

Contact email: [jloughlin@maehc.org](mailto:jloughlin@maehc.org)