Partnerships for Care

HIV TAC TEAM

Electronic Health Records, Session #3, Community of Practice

Presenters: Nancy Tabarangao, John Cupples & Diana Erani

24 May 2016

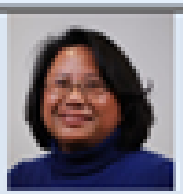
Protecting Electronic Health Records: Data Security and Integrity of e-PHI

MLCHC Webinar
Tuesday, May 24, 2016
1:00pm – 2:00pm

John Cupples
Nancy Tabarangao

Massachusetts League
of Community Health Centers

Presenters

	**John Cupples** John has extensive healthcare management experience in community health, long term care and hospital settings. Specialties include leadership, governance, project management, strategy, Meaningful Use, and ePHI protection.
	**Nancy Tabarangao** Nancy brings years of community health center management and consulting experience. Her areas of focus include planning, Meaningful Use, Workflow design, and process improvement.

Topics

- HIPAA Overview
  - The Privacy Rule
  - The Security Rule
  - The Breach Rule
  - The Patient Safety Rule
- Explore "PHI" (Protected Health Information)
- Protecting PHI (Risk Analyses)
- Breaches
- Audit Preparation
- State Law

Overview of HIPAA

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by Congress to establish a national framework for security standards and protection of confidentiality with regard to health care data and information.
- The goal of HIPAA is to protect patients' confidentiality while enabling healthcare organizations to pursue initiatives that further innovation and patient care.
- Before HIPAA there was no universally recognized security standard or basic mandates for Protected Health Information (PHI).

Overview of HIPAA (cont'd)

- There are four major provisions of HIPAA:
  - **Privacy Rule:** Standards for use and disclosure of PHI
  - **Security Rule:** Technical and non-technical security standards for protecting **electronic PHI** (e-PHI)
  - **Breach Notification Rule:** Framework for reporting breaches of unsecure PHI
  - **Patient Safety Rule:** Protects against increased liability risk when reporting patient safety or health care quality issues
- In 2009, privacy and security protections were expanded under the American Recovery and Reinvestment Act (ARRA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act to promote adoption and use of EHRs.

Overview of HIPAA (cont'd)

- Under the HITECH Act:
  - Rules were established for ensuring protection of e-PHI, and
  - Assessing security risks and establishing policies and procedures for protecting e-PHI became core requirements of the EHR Incentive Program and Meaningful Use.
- It is worth noting that the Meaningful Use program audit work plan sets as a goal that one in four eligible providers participating in the program are to be audited. So far, the primary reason for negative findings against eligible providers has been failure to comply with HIPAA.

The Four Major Provisions of HIPAA

The HHS Office for Civil Rights (OCR) is responsible for administering and enforcing, the major provisions of HIPAA.

- The **HIPAA Privacy Rule** protects the privacy of individually identifiable health information or PHI by establishing standards for the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their health information is used.

The Four Major Provisions of HIPAA (cont'd)

- **The HIPAA Security Rule** establishes a national set of security standards for protecting certain health information that is held or transferred in **electronic** form.
- **The HIPAA Breach Notification Rule** requires covered entities and business associates to provide notification following a breach of unsecured protected health information.
- The confidentiality provisions of **the Patient Safety Rule** protect identifiable information being used to analyze patient safety events and improve patient safety.

HITECH Act of 2009

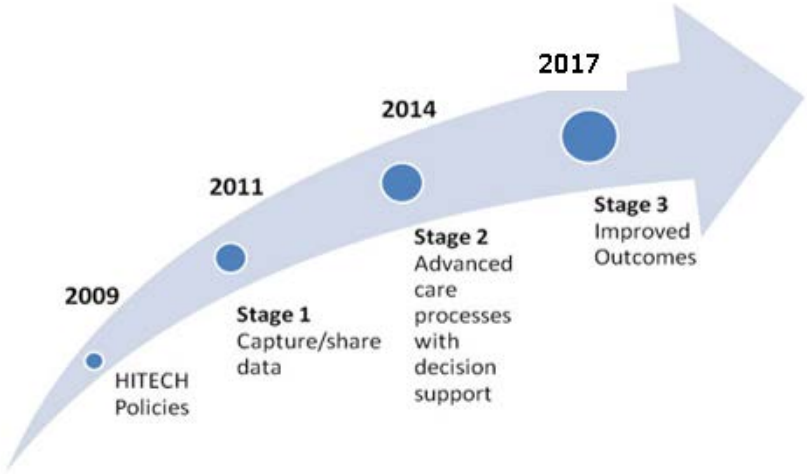
- The scope of privacy and security protections under HIPAA was broadened in 2009 when the HITECH Act was signed into law on February 17, 2009. The **HITECH Act**:
  - Was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology.
  - Addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

HITECH Act of 2009 (cont'd)

- Under the HITECH Act, the EHR Incentive Program was established to provide incentive payments to Eligible Professionals, Eligible Hospitals and Critical Access Hospitals to adopt, implement, upgrade and demonstrate the meaningful use of certified electronic health record (EHR) technology. This includes the core requirement for protecting e-PHI as of Stage 1.

Meaningful Use Stages of EHR Adoption and Use:

- Stage 1: Focuses on Data Capture and Sharing (2011)
- Stage 2: Focuses on Advanced Care Processes with Decision Support (2014)
- Stage 3: Focuses on Improved Outcomes (2017)



HIPAA: Privacy and Security

- **The Security Rule operationalizes the protections contained in the Privacy Rule** by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).

HIPAA: Privacy and Security (cont'd)

The Privacy Rule

- Focuses on the right of an individual to understand and control the use of his or her personal information: PHI should not be divulged or used by others against an individual's wishes.
- Covers the confidentiality of PHI in all formats including electronic, paper and oral.
- Assures that PHI will be safeguarded from unauthorized disclosure while allowing the flow of health information to provide and promote high quality health care.

The Security Rule

- Focuses on **administrative**, **technical** and **physical safeguards** of e-PHI.
- Protects e-PHI that is created, received, used or maintained by a covered entity. This includes e-PHI that is external or internal, stored or in transit.
- Promotes the integrity and availability of e-PHI.
  - Integrity: e-PHI is not altered or destroyed in an unauthorized manner.
  - Availability: e-PHI is accessible and usable on demand by an authorized person.

HIPAA: The Security Rule

- The Security Rule establishes standards for protecting certain health information that is held or transferred in electronic form, such as an EHR.
- A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing **covered entities** to adopt new technologies to improve the quality and efficiency of patient care.
- "Covered entities" under the Security Rule include health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA.

HIPAA: The Security Rule (cont'd)

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.
- Specifically, covered entities must:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce.

HIPAA: The Security Rule (cont'd)

- In addition to the PHI safeguards required by covered entities, they must obtain assurances from "Business Associates" - persons or entities that perform functions or activities that may involve use or disclosure of PHI on behalf of the covered entities – that they, the business associates, will appropriately safeguard PHI.

What is PHI or Protected Health Information?

- PHI is any individually identifiable health information or information that is a subset of health information, including demographic information, that is collected from an individual and is created or received by a covered entity and that relates to the individual's past, present, or future physical or mental health condition or any other information that can be reasonably used to identify the individual.
- The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

Common examples of PHI

Common examples of PHI:

- Names
- Addresses
- Dates (birth, admission, discharge, death)
- Telephone and fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Full face photographic images and any comparable images
- Certificate/License and account numbers

Information excluded as PHI

- Individually identifiable health information excluded as PHI includes:
  - Employment records held by a covered entity in its role as employer
  - Education records covered by the Family Educational Rights and Privacy Act

Key Provisions for Safeguarding PHI

- As noted previously, the HIPAA Security Rule requires that covered entities provide safeguards for protecting e-PHI. To help covered entities assure the confidentiality, integrity, and availability of all e-PHI, series of administrative, technical and physical security procedures have been established. **The key elements of the Security Rule include:**
  - Risk Analysis and Management
  - Administrative, Physical and Technical Safeguards
  - Organizational Requirements
  - Policies and Procedures and Documentation Requirement

Key Provisions for Safeguarding PHI (cont'd)

- **Establishing policies and procedures** to address the safeguards is key to ensuring that e-PHI is secure and mitigates risk for potential breach or unauthorized disclosure of e-PHI.
- **On-going review and update** of policies and procedures for compliance with the HIPAA Security Rule is required.
- **Conducting a security risk analysis** – a key element of the Security Rule – is a core measure for achieving meaningful use for the CMS EHR Incentive Programs. Failed audits for the EHR Incentive Programs have been primarily due to inadequate security risk analysis and documentation.

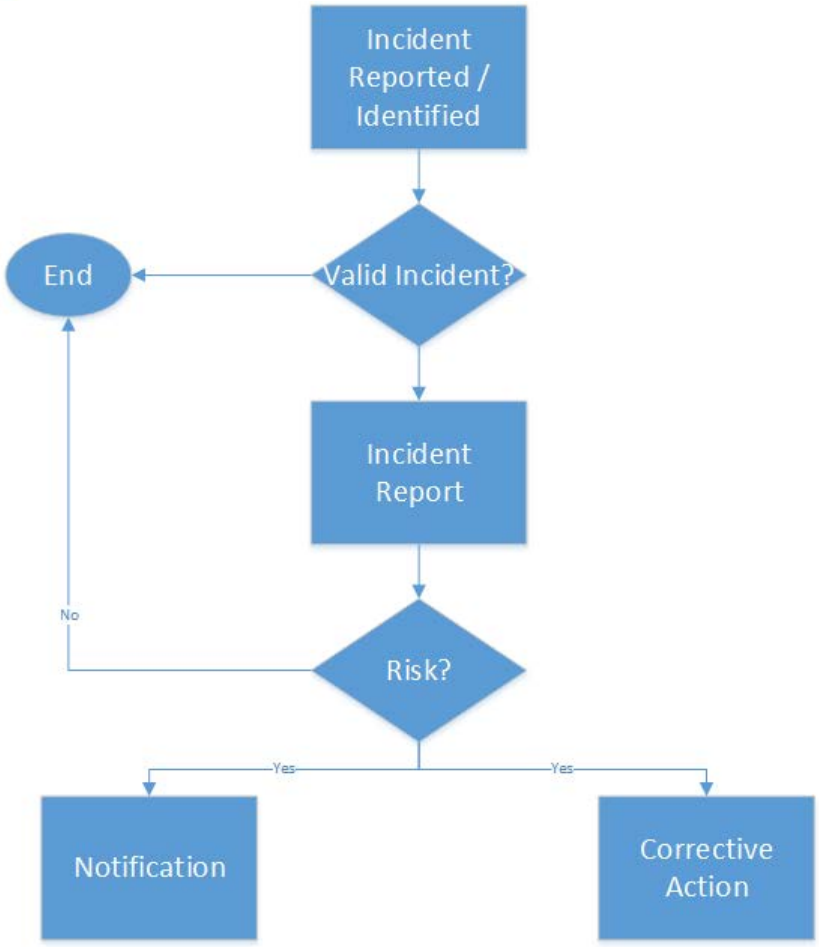
Risk Analysis and Management

- At minimum, a security risk analysis must be conducted annually, and if a security incident occurs.
- The analysis process must include:
  - Review of administrative, physical and technical safeguards in place to ensure e-PHI is secure.
  - Documentation of findings and an assessment of risk for unauthorized disclosure or use and/or breach of e-PHI.
  - A risk mitigation plan that documents the measures that will be taken to address the findings and the rationale for doing so.
  - Maintaining continuous, reasonable and appropriate security protections.

PHI Breach: What Next?

- Definition of Breach
  - A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
- Reporting of Breaches: All breaches must be reported to HHS.
  - **Individual.** Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information within 60 days.
  - **Notice to the Secretary.** In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and completing the Breach Notification form. (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)
  - **500 or more records:** Reported within 60 days after the breach.
  - **Less than 500 records:** Reported annually and no later than 60 days after the end of the calendar year.

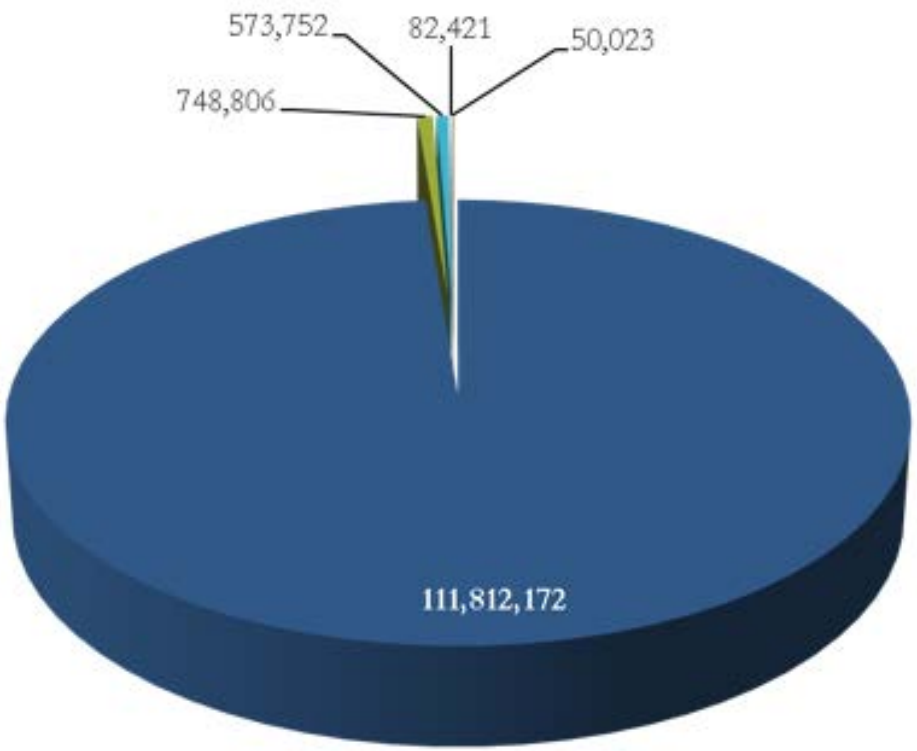
Breach Reporting



- Compromise the security and privacy of the PHI" means that the breach poses a significant risk of financial, reputational or other harm to the individual.
- The four factor risk assessment includes:
  - The nature and extent of PHI involved;
  - To whom the disclosure was made;
  - Whether the PHI was actually viewed or acquired; and
  - The extent to which the risk to the PHI has been mitigated.

2015: Breaches by the Numbers

268 Breaches with over 500 Records Breached: 113,267,174 Records Stolen

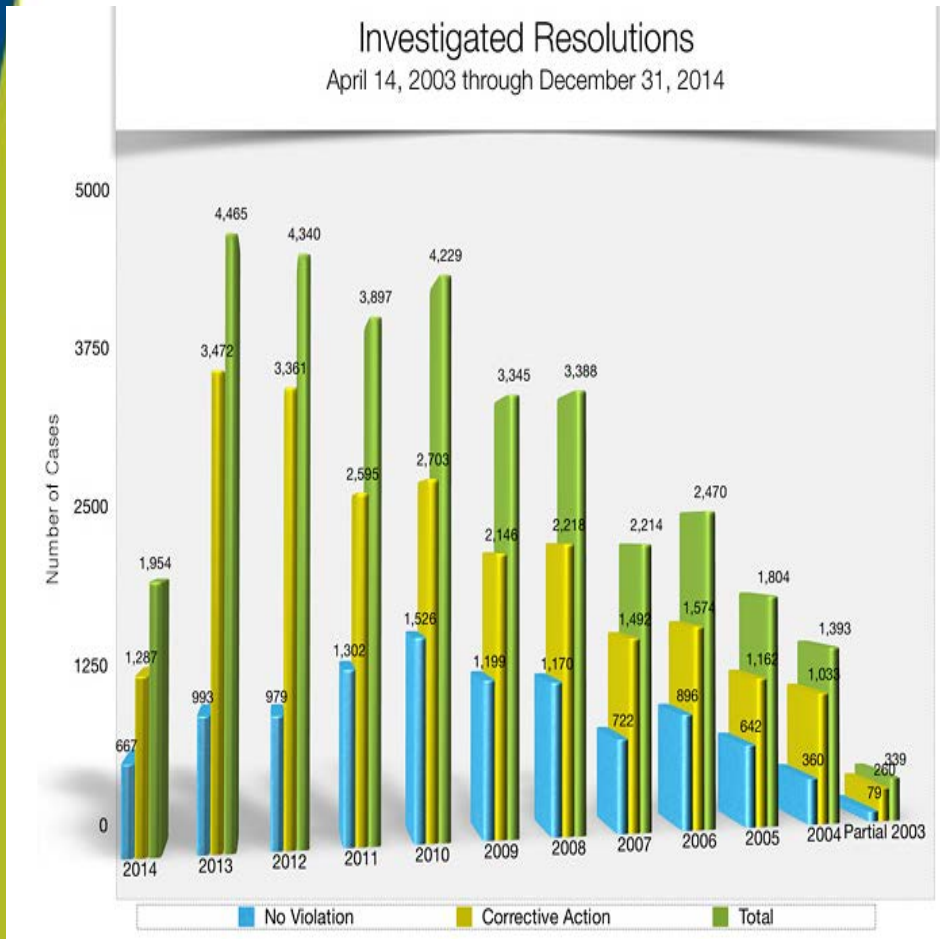


- **Stolen by external hacks, 111,812,172**
- **By other forms of theft, 748,306**
- **By unauthorized access or disclosure, 573,752**
- **Improper disposal of records, 82,421**
- **Records lost, 50,023**

This is equivalent to almost 1 in 3 Americans!

Source: CMS "wall of shame."
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HIPAA Enforcement



Year	Cases Investigated	Corrective Action	Percent w/ Sanctions
2004	1,393	1,035	74.3%
2005	1,804	1,162	64.4%
2006	2,470	1,574	63.7%
2007	2,214	1,492	67.4%
2008	3,388	2,218	65.5%
2009	3,345	2,146	64.2%
2010	4,229	2,703	63.9%
2011	3,897	2,595	66.6%
2012	4,340	3,361	77.4%
2013	4,465	3,472	77.8%
Total	**31,545**	**21,758**	**68.5%**

Source:
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html

Requirements if OCR Comes Calling!

You must be able to document (Note 6-yr. lookback):

- An organized and compliant risk management program reviewed at least annually.
- Policies and procedures:
  - Updated annually.
  - Tied to HIPAA requirements.
- Breach policy and procedures and demonstrated effective implementation plan.
- Technical capabilities to protect PHI must be updated on an ongoing basis.
- Disaster recovery and business interruption plan with appropriate policies and procedures.
- A "culture of security."

Check State Law Requirements

- All States have some law and regulation regarding the protection of private and personal information.
- Most States conform to HIPAA Privacy and Security requirements.
- But variations do exist. Compliance is required with the most stringent of State or Federal regulation.
- Your policies and procedures should reference both State law and Federal regulation.
- Where variances do exist, specific language should be included in your policies and procedures.

Resources for Further Information

- Go to the website to obtain a more detailed understanding of HIPAA. Also contains a variety of resources. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

- NACHC Information Bulletin, August 2013, *Four-Factor Risk Assessment for Determining Whether PHI Has Been Compromised*

- AHIMA. "Integrity of the Healthcare Record: Best Practices for EHR Documentation." *Journal of AHIMA* 84, no.8 (August 2013): 58-62. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050286.hcsp?dDocName=bok1_050286

HIV data transmission practices in Massachusetts

May 24, 2016

Diana Erani, Presenter

Massachusetts League
of Community Health Centers

HIPPA vs state laws

- HIPPA is a federal law that is broad
- State law is more protective of privacy
- Whichever is more protective preempts the less restrictive laws

Federal and state laws for HIV data transmission

HIPPA codifies protected health information (PHI) under 45 CFR § 160.103.

Massachusetts codifies HIV testing data under MGL 111 § 70F.

Massachusetts HIV Testing Statute

- Strict Protection for Disclosure of HIV Testing Results:
  - "A facility…, physician or health care provider shall not (1) test any person for the presence of the HIV antibody or antigen without first obtaining that person's verbal informed consent; (2) disclose the results of such test to any person other than the subject of the test without first obtaining the subject's written informed consent; or (3) identify the subject of such tests to any person without first obtaining the subject's written informed consent. A written consent form shall state the purpose for which the information is being requested and shall be distinguished from written consent for the release of any other medical information"

Massachusetts HIV Testing Statute

- Exception for Disclosure to Massachusetts Department of Public Health

  "The Massachusetts HIV Testing Statute does include an exception for reporting HIV test results to the Massachusetts Department of Public Health see M.G.L., c., 111, §70F. This reporting is required under 105 CMR 300.000: *Reportable Diseases, Surveillance and Isolation and Quarantine Requirements.* However, it is important to note that this exception *only* applies to the Mass DPH and not to other state or local departments or programs, unless these departments or programs can show evidence of legislative permission to do so.

  Source: Hemenway & Barnes

Massachusetts HIV Testing Statute

Written Informed Consent Required for Release of Testing Information Obtaining written consent to care generally includes a release of medical information to insurers (for billing purposes) or to other treating providers and is generally obtained during the initial engagement to care. The revised c. 111, § 70F defines "written informed consent" as a written consent form for each requested release of the HIV test results.

Source:
http://www.mass.gov/eohhs/docs/dph/aids/routine-hiv-screening-clinical-advisory.pdf

Massachusetts HIV Testing Statute

The law does not specify who may obtain the consent to release this information. Generally local practice or institutional protocols dictate who obtains consent for release of information – it may be office staff or clinical staff. All individuals diagnosed with HIV infection should have the option to receive optimal medical care. This is achieved when all clinical providers treating an individual have appropriate legal access to medical information.
Source:
http://www.mass.gov/eohhs/docs/dph/aids/routine-hiv-screening-clinical-advisory.pdf

Massachusetts HIV Testing Statute

MDPH strongly recommends the use of distinct and separate HIV test results release consent language within the general consent document when a general consent for release of test results or medical records is employed (see model informed consent language). The release must state to whom or to where the test results will be released. The recipient(s) of the information should be identified as a provider of care appropriate for that patient.

Source:
http://www.mass.gov/eohhs/docs/dph/aids/routine-hiv-screening-clinical-advisory.pdf

Information that may contain HIV status

- Laboratory data
- Medication lists
- Allergy lists
- Appointment information
- Insurance information
- Social history

What does this mean for the grant?

- HIV data can and should be reported to the Massachusetts Department of Public Health as a condition of participating in this grant.
- HIV data should not be transmitted for other purposes without the written consent of the patient. This consent must include the purpose of transmission and to whom the data will be transmitted each time the data is shared outside of the healthcare entity.
- The privacy laws make care coordination more cumbersome for HIV patients.

Thank You

Diana Erani, MBA is the director of the Health Center Controlled Network at the Mass League of Community Health Centers. She is the former Chief Operating Officer of a Community Health Center and has experience in different healthcare management settings.

Good health. Right around the corner.

40 Court Street, 10th Floor
Boston, MA 02108
ph 617-426-2225
www.massleague.org

Massachusetts League
of Community Health Centers

Partnerships for Care

HIV TAC TEAM

REGISTER FOR SESSION #4

Tuesday, June 28

1:00 – 2:15 PM EDT

https://attendee.gotowebinar.com/register/5094375293892947457

MayaTech® Corporation

Vision | Integrity | Knowledge | Solutions

Partnerships for Care

HIV TAC TEAM

WE NEED YOU!

Participate as Health Center co-presenter.

Contact:
Victor Ramirez,
P4C HIV TAC Collaborative Training Coordinator
vramirez@mayatech.com

Partnerships for Care

HIV TAC TEAM

Thank you for participating in this Webinar.
We hope that you are able to find the information provided useful as you continue your P4C project.
We ask that you take a few moments to complete the feedback survey you will receive when you close out of this webinar.

Partnerships for Care

HIV TAC TEAM

Thank you for participating in today's webinar

If you have any additional questions, please email us:
P4CHIVTAC@mayatech.com

MayaTech® Corporation

Vision | Integrity | Knowledge | Solutions