Effective Tips for Implementing a Successful Privacy & Information Security Program

Alexander D. Eremia, JD, LL.M.
Vice President, Deputy General Counsel and Chief Privacy Officer
MedStar Health, Inc.

Shallie Bryant
Privacy Manager, MedStar Health, Inc.

Promoting Trust by Protecting Privacy®

MedStar Health

Is this your privacy and security awareness program?

MedStar Health

TRUSTED LEADER • CARING FOR PEOPLE • ADVANCING HEALTH

About MedStar Health

- $3.9 billion non-profit, regional healthcare system
- 9 hospitals/healthcare services in the Mid-Atlantic Region
- 3,300 licensed beds
- 26,000+ associates
- 5,300+ affiliated physicians
- 162,000+ inpatient admissions per year
- 1.5 million+ outpatient visits each year

As of 6/30/10

Organization

- Affiliated Covered Entity ("ACE")
  - Chief Privacy and Security Officers
  - Single Notice of Privacy Practices
  - Enhances ability to share/use PHI across system
  - Requires centralized governance structure
  - Requires standardized
    - Training and education
    - Privacy investigations and responses
    - Disciplinary measures
  - ACE liability

What does security mean?

What does privacy mean?

MedStar Health

The Trusted Leader in

Caring for People

and Advancing Health

Key Objectives

- Infrastructure
- Patient trust = patient satisfaction
- All confidential information
- Compliance with laws
- Reputation as industry leader in privacy and information security practices

Strengths

- Strong privacy department leadership and technical expertise
- Staff informed and passionate
- Successful history and familiarity with using a variety of communication tools
- Availability of external resources
- External consultants to assist with communications
- Liaisons/champions throughout system

Weaknesses

- Limited staff
- Many priorities with overlapping deadlines
- Lack of infrastructure
- Highly regulated industry with extensive “mandatory” education requirements
- Messages may compete with other internal campaigns
- Technology moving faster than policy

Opportunities

- Internal platforms such as
  - Intranet for expanding resources and testing new tools
  - Email communications
- "Privacy and Security" is a big issue
- Growing awareness and public interest
- Potential to be a resource on privacy and information security to patients and other organizations

Threats

- Violations getting more attention
- Stronger enforcement of regulations
- Potential negative ramifications to reputation and bottom line
- Heightened scrutiny of privacy and security incidents and focus on patient rights
- Increased exposure due to new regulations
- Potential budget constraints

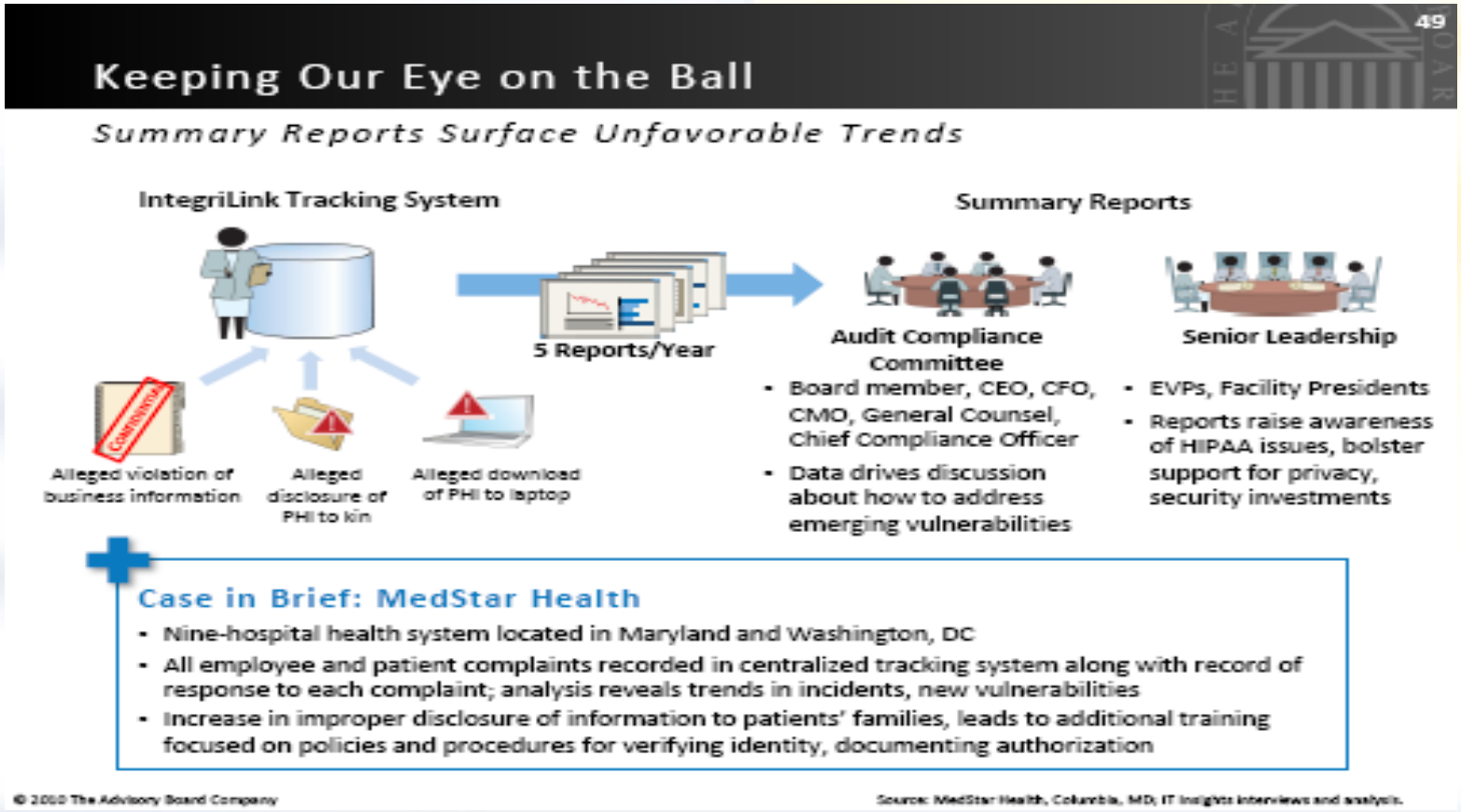
SMART Goals

- Publish updated corporate privacy and security policies by January 1, 2009
- Develop and roll out new privacy and security training modules by June 30, 2009
- Raise and maintain awareness in the MedStar community; measure annually
- Demonstrate effectiveness of program by monitoring:
  - Employee test scores on mandatory training
  - # visits to Intranet site
  - # and type of employee violations
  - Ordering of privacy printed materials

Using Data Analysis to Identify Trends

- Employee and patient complaints recorded in centralized tracking system that tracks
  - Trends in incident
  - New vulnerabilities

Snapshot - Data Analysis Captured cont.



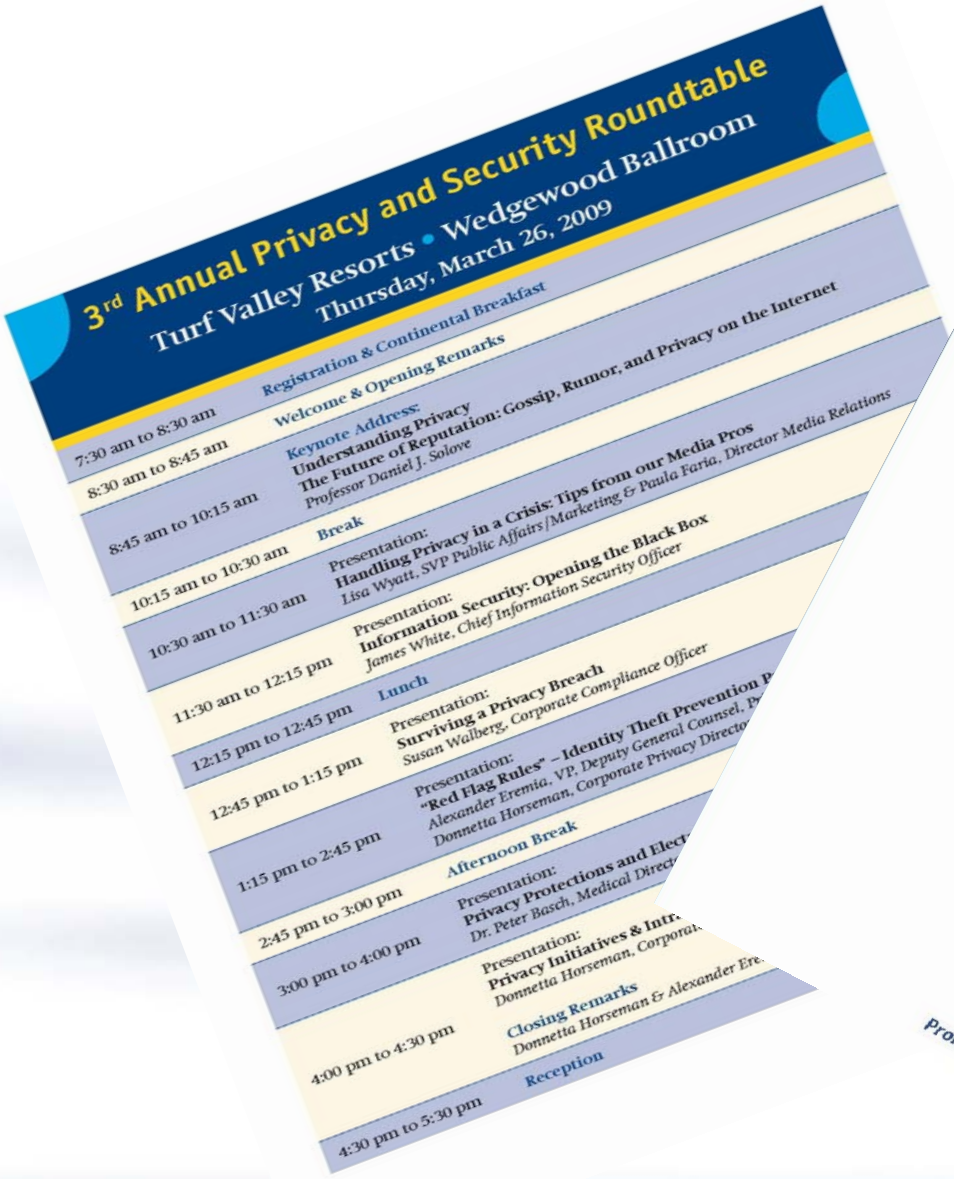
Tips for Nipping Non-Compliance in the Bud

Privacy Week Re-Training

- Conducted at each facility
- Reviewed protocol for disclosing information, verifying identity of requestor
- Used opportunity to underscore criticality of compliance, repercussions of HIPAA violations

HIPAA Brochure

- Distributed to all 25,000 employees
- Contains step-by-step instructions for releasing deceased patients' information, guidelines for disclosing information to patients' family members
- Provides instructions for how to report suspected breaches



3rd Annual Privacy and Security Roundtable

Turf Valley Resorts • Wedgewood Ballroom

Thursday, March 26, 2009

7:30 am to 8:30 am	Registration & Continental Breakfast
8:30 am to 8:45 am	Welcome & Opening Remarks
8:45 am to 10:15 am	Keynote Address: **Understanding Privacy** **The Future of Reputation: Gossip, Rumor, and Privacy on the Internet** *Professor Daniel J. Solove*
10:15 am to 10:30 am	Break
10:30 am to 11:30 am	Presentation: **Handling Privacy in a Crisis: Tips from our Media Pros** *Lisa Wyatt, SVP Public Affairs/Marketing & Paula Faria, Director Media Relations*
11:30 am to 12:15 pm	Presentation: **Information Security: Opening the Black Box** *James White, Chief Information Security Officer*
12:15 pm to 12:45 pm	Lunch
12:45 pm to 1:15 pm	Presentation: **Surviving a Privacy Breach** *Susan Walberg, Corporate Compliance Officer*
1:15 pm to 2:45 pm	Presentation: **"Red Flag Rules" – Identity Theft Prevention P** *Alexander Eremia, VP, Deputy General Counsel, P* *Donnetta Horseman, Corporate Privacy Directo*
2:45 pm to 3:00 pm	Afternoon Break
3:00 pm to 4:00 pm	Presentation: **Privacy Protections and Elec** *Dr. Peter Basch, Medical Direct*
4:00 pm to 4:30 pm	Presentation: **Privacy Initiatives & Intr** *Donnetta Horseman, Corporat* Closing Remarks *Donnetta Horseman & Alexander Ere*
4:30 pm to 5:30 pm	Reception

Are You "In The Know?"

MedStar Heal

Are you up-to-date on the recent changes to the HIPAA Privacy laws?

Make sure you are "in the know" and prepared to protect our patients by attending MedStar Health's 4th Annual Privacy & Security Roundtable Event.

Thursday, April 1, 2010
Sheraton Columbia Town Center Hotel in Columbia, Maryland

Do you deal with protected health information as a MedStar associate? Are you a supervisor in patient care, a privacy liaison, a HIM professional, or work in administration or communications? **You cannot afford to miss this important event.**

The day's agenda is jam-packed with special guest speakers, expert presenters and information on all the latest news and changes to healthcare privacy and security, including:

- HITECH's impact on privacy and security
- anatomy of a breach, notification, risk assessment
- privacy implications of MedStarConnect
- the link between privacy and security
- privacy and security implications for RHIOs
- social networking and privacy
- department updates and much more!

Attendance is free and open to all MedStar Health workforce members. Space is limited, so **register via Sitel by March 29**, please feel free to contact Shallie Bryant (410-772-6548 or shallie.bryant@medstar.net) with questions or requests for additional information. Breakfast and lunch will be provided, and the day will conclude with an afternoon reception. Breakfast and registration opens at 7:30 a.m. and the conference will start promptly at 8:30 a.m.

Registration instructions:

- log on to Sitel at http://www.web.sitelms.org
- once logged in, click "calendar of events"
- go to **Select Organization**
- select **MedStar Corporate MD**
- go to the month of April

Promoting Trust by Protecting Privacy™

MedStar Health

TRUSTED LEADER • CARING FOR PEOPLE • ADVANCING HEALTH

Do you know the answers to these questions?

What is a breach? When is a patient authorization form needed? How can I spot a red flag? Is it wrong to look at my own medical record? What does encryption mean?

Do you know the answers to these questions? As an associate of MedStar Health, you need to understand the laws and policies surrounding protected health and confidential business information. Protecting our patients' privacy, securing PHI, and safeguarding business information are critical to our organization's success as the region's Trusted Leader in Caring for People and Advancing Health.

MedStar Health's Corporate Privacy Department is celebrating Health Information Privacy and Security Week, April 12-17. Privacy leaders are visiting our hospitals and presenting an educational session to associates, covering basic privacy and security rules and new developments to the privacy laws.

Join us during Privacy and Security Week to get your questions answered, refresh your memory on the rules and regulations, and even learn something new. And by attending and taking an online quiz after the session, you can be entered to win prizes, including the iPod grand prize. (More details will be provided at the session.)

Associates should register via SITEL: http://www.web.sitelms.org (Select Organization, select MedStar Corporate MD, then go to the month of April). Associates can register at any one of the MedStar locations listed below. Seating will be limited and light refreshments will be served.

Health Information Privacy and Security Week, April 12-17

date	*location*	*time*
April 12	Franklin Square Hospital Center (Kotzen Room)	10-11 a.m.
April 12	Good Samaritan Hospital (Parker 3)	1-2 p.m.
April 13	Harbor Hospital (Teleconference Room/Baum Conference Center)	9-10 a.m.
April 13	National Rehabilitation Hospital (Managers Forum)	12-1 p.m.
April 14	Washington Hospital Center (GME Conference Room)	12-1 p.m.
April 15	Georgetown University Hospital (Martin-Marietta Lombardi Cancer Center)	12-1 p.m.
April 16	Union Memorial Hospital (Main Conference Room)	9-10 a.m.
April 16	Montgomery General Hospital (Community Learning Center)	12:30-1:30 p.m.

Additional dates and locations are being scheduled, a second announcement will be sent when details are finalized.

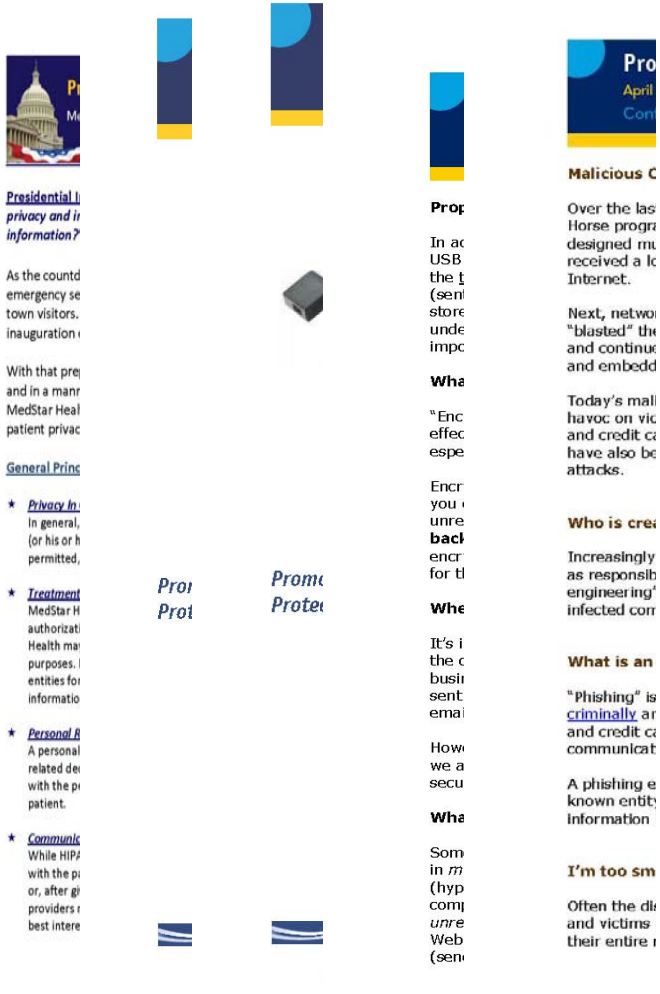
Questions? Please contact your facility's privacy liaison or Shallie Bryant (410-772-6548 or shallie.bryant@medstar.net).

Promoting Trust by Protecting Privacy™

MedStar Health
Corporate Privacy Department

MedStar Health

TRUSTED LEADER • CARING FOR PEOPLE • ADVANCING HEALTH



MedStar Health

HEALTH INFORMATION PRIVACY AND SECURITY WEEK
APRIL 8 - 14
KEEPING IT PERSONAL – HEALTH INFORMATION YOU CAN TRUST

Sending Electronic Protected Health Information (ePHI) Securely

ePHI and other sensitive data can only be transmitted by permitted methods to outside entities that are authorized to receive the data. In cases where ePHI is disclosed to a business associate, vendor, etc., a signed MedStar Health business associate's agreement addendum is required. Moreover, ePHI and other sensitive data must be protected while being transmitted to external partners via the Internet. While there are many ways to secure data transmissions, MedStar Health currently has three primary methods:

- **Secure e-mail**. This is the best option for sending Protected Health Information (PHI), sensitive data or small file attachments that contain ePHI. To send a secure (encrypted) e-mail from Lotus Notes, simply type **[Encrypt]** in square brackets at the beginning of the subject line of your email message. You can then add the remainder of the text in the subject line, complete the body of the message, and attach any files. By virtue of the **[Encrypt]** tag at the beginning of the subject line, the system will automatically send the e-mail to the secure e-mail server for delivery. Receivers of the secure e-mail will need an Internet connection, Internet browser, e-mail address, and complete a simple registration process to set up their e-mail address with a password of their choosing. Typically, no special setup or technical assistance is necessary to send secure e-mail. Since the secure account is specific to the receiver's e-mail address, this method can be used for all future, subsequent secure messages without having to set up a new account.

- **Secure File Transfer**. This is the best option for sending large files, large collections of smaller files or file attachment types that may be blocked by MedStar Health or the receiver's e-mail system (e.g., .exe and .com – executable files, etc.). Setup is required for this option and users should contact the help desk to arrange for assistance in setting up secure file transfers.

- **Interface Engine**. This is the best option for setting up routine file transmissions with external partners and especially well suited for automated, machine-to-machine communications. A good example of when the interface engine would be the best option is the need to send monthly payroll data to an external partner for processing. The interface engine will manage and secure the file transmission process and ensure that the transmission is completed in the event there is an interruption. Again, setup is required for this option and users should contact the help desk to arrange for assistance in setting up file transfer via the interface engine.

Protecting health information and sensitive MedStar Health data is the responsibility of all MedStar Health employees and affiliates. Please ensure all transmissions of ePHI and sensitive MedStar Health business data to external partners are protected. Contact the help desk for additional assistance.

Look for Thursday's installment of the Privacy and Security Week Information Series, which will focus on protecting electronic resources.

Alexander D. Eremia, J.D., LL.M.
Associate General Counsel and

Strategies

- Communication & Awareness
  - Memorable, high-impact visuals
  - Customize messages for audience
  - Keep materials positive in tone, tied to *promoting trust*
  - Group various materials under like themes

Strategies

- Training
  - Develop role-based modules that focus on concepts applicable to position
  - Integrate visuals and messages into all communication and training materials
  - Consistency

Steps to Success

MedStar Health

TRUSTED LEADER • CARING FOR PEOPLE • ADVANCING HEALTH

Steps to Success

- Assess
  - Areas of confusion? concerns? frequent trouble spots?
  - Benchmark current position
- Plan
  - Mission, vision, values
  - Major goals and objectives
  - Strategies to accomplish goals
  - Measurements of success

Steps to Success

- Implement
  - Develop theme and key messages
  - Utilize existing communication channels to their fullest potential
  - Work in cooperation with your internal communications staff
  - Support your program needs with employee task forces, volunteer committees, and/or outside consultants
- Evaluate

Tools & Tactics

- Celebrate recognition weeks
- Host annual roundtable
- Be visible
- Saturate the market
- Frequency and variety
- Appeal to your audience

Protect valuable information with strong passwords, not celebrations.

Good passwords are easy for you to remember, but hard for others to guess. Use combinations of letters, numbers, and special characters for your passwords to protect confidential patient and business information. Contact the MedStar Health Service Desk for more tips on changing your password (410-933-HELP).

For more information about privacy issues, contact your facility's privacy liaison or visit the StarPort Intranet site. To anonymously report concerns or potential privacy violations, call 1-877-811-3411.

Promoting Trust by Protecting Privacy™

MedStar Health

Tools & Tactics

- Show employees you care
- Educate/inform about personal privacy issues
    - Travel safety
    - Online safety for kids/teens
    - Holiday shopping

Tools & Tactics

- Seek feedback from your audience
  - Tailor/improve messages and strategies
- Consider rewards and incentives
- Make resource materials readily available
- Be creative!
- Always include a call to action or a direction for more information
- Be as interactive as possible
- Be POSITIVE!

Don’t have a big budget?

- Think big return, for small cost
  - Lunch and learns
  - Low-cost give aways
  - Use employees for “models” and ambassadors
  - Games, trivia contests
  - Site visits by experts
  - Use existing communication resources
  - Be repetitive
  - Food is an attention getter
  - Use supervisors/front line managers as communicators

Why do you need a budget?

Do's and Don't's

- **DO**
  - Be positive
  - Measure
  - Know your audience
  - Develop a strategy
  - Ask for help
  - Get buy-in from senior management
  - Ask for a budget
- **DON'T**
  - Equate "campaign" with "program"
  - Equate "awareness" with "training"
  - Use only one or two channels to communicate
  - STOP

This is not a one-time effort !

Questions?

Email: alexander.d.eremia@medstar.net
or privacyofficer@medstar.net

Promoting Trust by Protecting Privacy®

MedStar Health