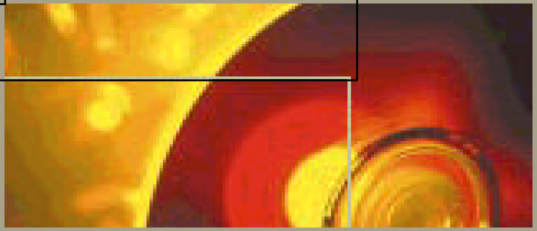
convergence

Privacy & Security Compliance for the System Vendor

June 22, 2001

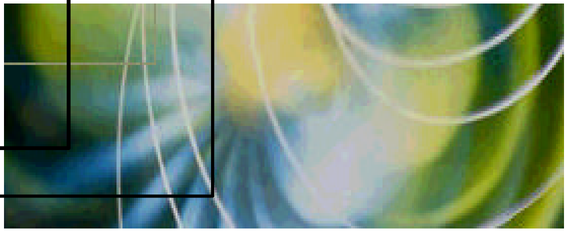
TRIZETTO®
enabling health ebusiness℠

Roadmap to HIPAA Compliance



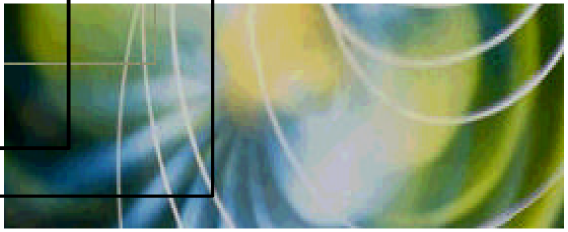
How to Get from Where You Are to Where You Ought to Be …

Why Comply?



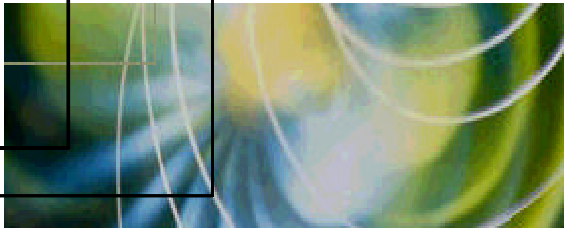
- Contractual agreements with clients
- Market place realities
- It’s the right thing to do

HIPAA Presents Challenges for Vendor



- Had to start early to be ahead of implementation curve of clients
- Large investment in R&D to enhance systems and processes well in advance of client adoption means delayed ROI
- Awareness raising and education – "Why me?" syndrome

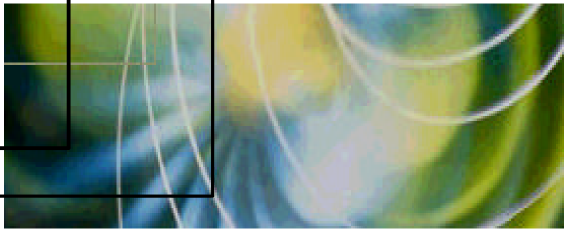
TriZetto's HIPAA Commitment



Total commitment to HIPAA compliance throughout entire organization

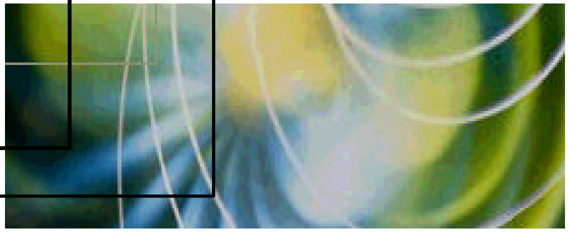
- ASP
- Clearinghouse/health plan activities
- Transactions services functions
- Business associate
- Software application vendor

What is our Approach?



- Multi-faceted organization wearing many different hats and so have had to approach compliance from many different perspectives
- HIPAA Compliance Office is the driving force in our efforts
  - Compliance office efforts supplemented by workgroups addressing specific HIPAA issues
  - HIPAA “champions” in workgroups coordinate compliance efforts within each segment of organization
- Compliance program began in 2000... continuing on in 2001...and 2002, 2003... and beyond

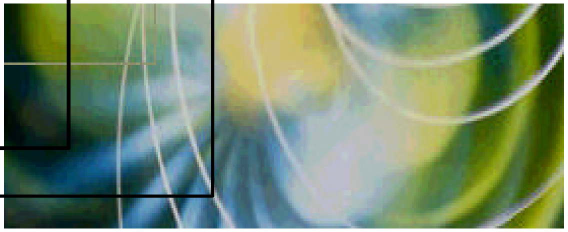
Step 1: Form a Compliance Team



Need a dedicated core team whose job *is* HIPAA

- HIPAA Compliance Office – two full time staff members dedicated to HIPAA compliance (third person coming soon)
  - Privacy Officer part of compliance office team
  - Separate Security office and Security officer and staff
- HIPAA “champions” from each business unit throughout organization

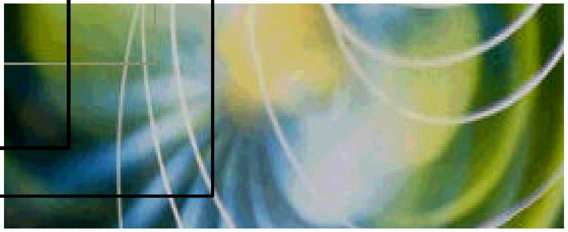
Step 2: Get Executive Buy-in and Support



Critical that HIPAA support begins at the top

- Executive Steering Committee (ESC) includes Senior VPs from every part of organization
- HIPAA Compliance Office reports to ESC
- Assures executive level support for assignment of time and resources to HIPAA projects
- Awareness and education activities start here

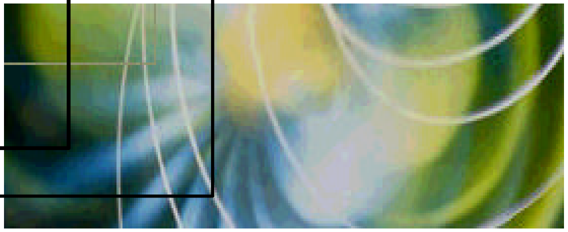
Step 3: Form HIPAA Workgroups



Form HIPAA workgroups from among HIPAA “champions” throughout organization

- Compliance Office leads and coordinates workgroups
- “All HIPAA” group tracks progress toward compliance with all rules
- EDI Taskforce addresses implementation issues related to electronic transactions and code sets; small workgroups focus on resolving specific EDI issues
- Privacy/Security Taskforce is responsible for developing and implementing Privacy/Security policies and procedures

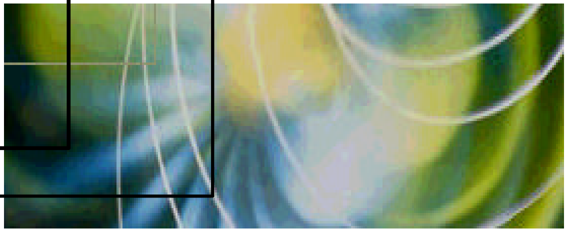
Step 4: Conduct HIPAA Assessments



Conduct HIPAA gap assessments and business impact analysis

- Use a systematic process can replicate
- Assess and reassess as organizations grows and changes
- Reach entire organization, even those departments that don't think HIPAA applies to them
- Run a "pre-assessment" to determine whether or not to assess farther

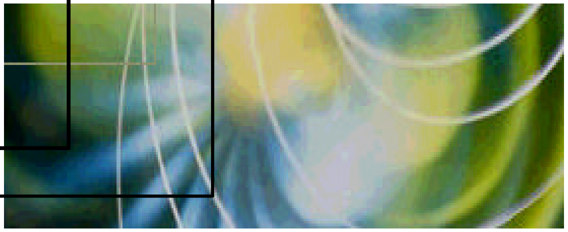
Step 5: Analyze Data



Analyze data and determine compliance gaps

- Develop strategies for compliance efforts
- Design overall solutions and approaches
- Create a shopping list of resources and materials
- Go back to the “top” for support for obtaining resources, materials and time

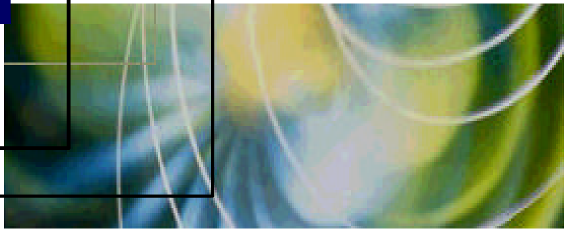
Step 6: Enlist Help of Human Resources



Design “Entrance to Exit” approach to HIPAA compliance

- Incorporate HIPAA into HR interactions - new employee orientation to exit interviews
- Include HIPAA awareness in employee training
- Add HIPAA policy and privacy agreement to employee handbook
- Coordinate termination procedures with IT
- Develop policies regarding sanctions for violations

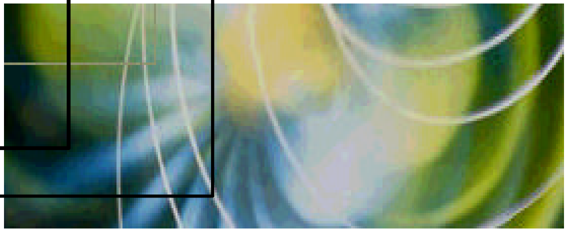
Step 7: Awareness and Educational Programs



Develop HIPAA awareness and education programs appropriate for your organization

- Offer short sessions on frequent basis – Lunch and Learn classes good options
- Take advantage of electronic training – web casts, audio casts, internet-based
- Provide general HIPAA awareness training plus focused training for Privacy and Security issues
- Plan to provide on-going training due to staff turnover and movement to new job responsibilities

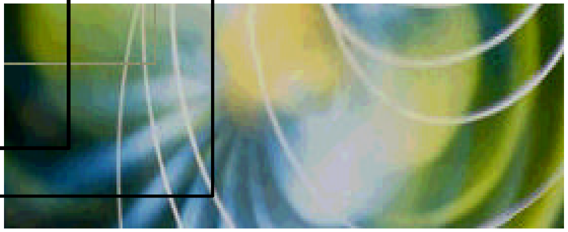
Step 8: Develop HIPAA Policies & Procedures



Compliance office begins by documenting corporate level policy and guiding principles

- Team leads and managers at unit level develop specific policies and procedures for their own departments
- Jump start process with policy and procedure workshops
- Focus first on areas handling protected health information (PHI) in day-to-day work
- Move next to support personnel (application and systems) and finally to entire company – everyone must get HIPAA!
- “Fix the problem not the blame” approach

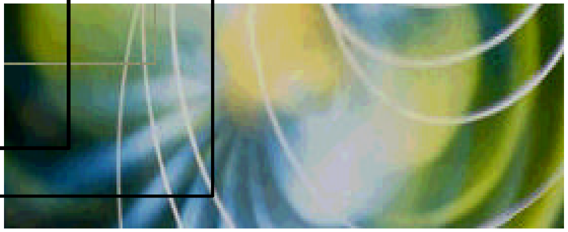
Step 9: Have Some Fun with HIPAA!



Put some fun and humor into HIPAA

- Make use of employee newsletter - HIPAA articles, cartoons, humor
- Create HIPAA posters – play off company theme for HIPAA and make posters attention grabbers
- Give out HIPAA trinkets to reward participation in HIPAA training sessions and activities
- Use screen savers with HIPAA messages
- “HIPAA knowledge” contests - with prizes

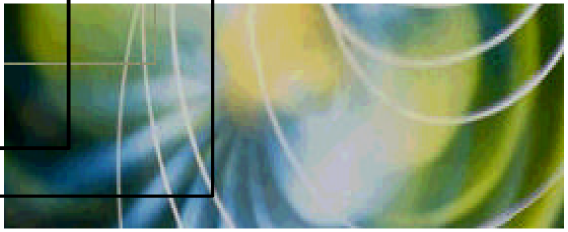
Step 10: Document, Document, Document



Must document - both Privacy and Security rules require documentation of policies and procedures

- Seek legal review of policies and procedures and documentation
- Look for independent certification of efforts and results – EHNAC, JCAHO, NCQA, etc.
- Make documentation easily available to staff
- Post policies and procedures on intranet
- Put a HIPAA Handbook in each work area

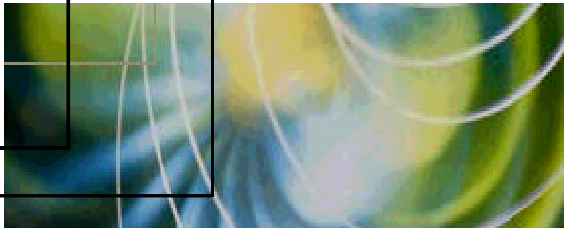
Step 11: Assess and Assess Again



You may never be "done" – will need to re-assess organization as it grows and changes due to

- Acquisitions
- New product lines
- Changes in corporate structure and roles
- Changes in regulations

Step 12: Maintain Compliance



HIPAA is not a one-time fix; compliance requires on-going monitoring

- Keep up with legislative changes - new regulations and modifications to existing rules
- Conduct “fire drills” to test your emergency security procedures – fix the problem, not the blame
- Conduct on-going compliance audits of physical security, access controls, and privacy practices
- Make sure termination procedures are strictly followed

convergence

Questions?