

Achieving Continuous HIPAA Compliance

Tips & Tricks

Gary Swindon
RiskWatch, Inc.

Achieving Compliance

- Compliance Rules & Characteristics
- The Keys to Achieving Compliance Goals
- The Other Interested Groups
- Steps to Creating a Common Focus-for Superior Results
- Sleeping Well at Night-or: 'Do You Know Where Your Data Is?'
- Compliance as a Way of Life

Compliance Rules & Characteristics

- Rule #1: If you believe that you can achieve compliance once-for all time; you are doomed and **YOU WILL FAIL!**
 - Decide to change your mindset now and the mindset of those around you
 - Be willing to look beyond HIPAA compliance and those who have been 'blessed' with Privacy & Security duties as a result

Compliance Rules & Characteristics-Continued

- Rule #2: Continuous compliance is a process not a destination.
 - The last person known to have a 'silver bullet' was the Lone Ranger
 - Success is going to involve many other people and functional areas

Compliance Rules & Characteristics-Continued

- Rule #3: If you believe that you can do it by yourself you need clinical help.
 - It truly does not matter how effective you are in your job-you are one person
 - You can be a beacon, a guide, and a focal point but others will determine your success

Compliance Rules & Characteristics-Continued

- Rule #4: Checklists are not compliance.
 - The most critical aspect of continuous compliance is risk assessment; without it you are flying blind (paragraph 164.308 requires both risk assessment and risk management)
 - You need a stable base from which to measure your success

The Keys to Achieving Compliance Goals

- As the song says: 'Get a plan Stan'
 - Document your goals and expected outcomes
 - Pay attention to the baseline HIPAA rules: but don't neglect other laws etc.
 - Identify those who will gain and lose from the effort
 - Get senior management buy in
 - Document the financial and organizational impacts from your efforts

The Keys to Achieving Compliance Goals-Continued

- Perform a good risk assessment:
 - Ideally, it should be quantitative not qualitative
 - The results should provide things you need:
 - Identify weaknesses, threats, & exposures
 - Identify mitigation efforts
 - Identify potential costs of mitigation
 - Identify the level of risk that the organization is willing to accept
 - Provide a stable 'baseline' from which to measure the impact of your efforts

The Keys to Achieving Compliance Goals-Continued

- Tie the desired outcomes to the efforts of others-where should help come from?
- Get resources committed to the process:
 - Management Support
 - People
 - Money
- Provide feedback and measurement

The Other Interested Groups

- Remember that there are others with a goal set similar to yours-and they can help:
 - Internal Audit
 - Information Security
 - Privacy Group
 - Patient Care Advocates/Patient Care Coordinators
 - Human Resources
 - Health Information Management etc.

Steps to Creating a Common Focus-for Superior Results

- Committees can help do the work
 - Standing Committees: Privacy, Security & Policy
 - Involve senior directors/managers-NOT VPs
 - Don't forget the clinical side
- Education focused on the common goals
 - Training, Education, Awareness; who gets what & when
 - Remember HIPAA says everyone gets educated; there are no exceptions

Joining and Combining Focus-for Superior Results-Continued

- Establish a HIPAA Privacy & Security Liaison Program:
 - Management level people
 - All areas of operations including food service
 - Assigned as an additional duty
 - Conducts quick checks on departments
 - No set schedule but set goals for the number of assessments
 - Collect the results and report them

Joining and Combining Focus-for Superior Results-Continued

- Participate in awareness events or become the catalyst for them:
 - AHIMA and others have a National Week declared for healthcare related activities
 - Combine observances such as Compliance Week etc. into a once a year activity
 - Set up a booth or table near cafeterias; give away prizes for completing compliance puzzles
 - Give away candy or key chains etc. ask questions at random on HIPAA issues

Joining and Combining Focus-for Superior Results-Continued

- Start a voluntary HIPAA assessment/evaluation program:
 - No blame activities; blame kills participation
 - Units can request the Privacy & Information Security Officer do a walk through
 - Educational support for on the spot corrections
 - Include 'Dumpster Diving' activities (sometimes called the latex glove approach)

Joining and Combining Focus-for Superior Results-Continued

- Tie the compliance program to the internal audit program:
 - The common basis for both should be the risk assessment process
 - Formalizes critical compliance monitoring as one more set of 'eyes & ears'
- Create & publish a Compliance Bulletin:
 - Privacy, Security, Compliance & Internal Audit news and tips: make it a resource for everyone

Sleeping Well at Night-or: 'Do You Know Where Your Data Is?'

- Acknowledge that most of your information is on or stored in a computer:
 - Technical evaluation of the IS/IT risk is also necessary
 - Tie the technical security manager to the Corporate Information Security Officer at least on a dotted line
 - Require regular monitoring and reporting on the technical risks to your information

Sleeping Well at Night-or: 'Do You Know Where Your Data Is?'

- Organize for success: (if possible)
 - Move Privacy, Security, Compliance & Internal Audit into the same organization
 - Have the organization report to the audit/or management committees of your board
 - Require quarterly reporting on all compliance activity to the full board
 - Give the organization its own legal counsel independent of any corporate legal group

Compliance as a Way of Life

➤ Remember:

- Your organization's size does not matter when it comes to compliance
- You can have a continuous compliance program but you have to work at it
- You cannot have an effective program without good risk assessments
- You have to be willing to try new ideas and you have to support them

Questions?

