Living with HIPAA: Compendium of Next steps from Rural Hospitals to Large Health Systems to Physician Practices

Presented by HIPAA Pros

5th Annual HIPAA Summit

Baltimore, Maryland

October 31. 2002

CHC Healthcare Solutions

HIPAA PROS.com

Living with HIPAA

- Implementation priorities
  - Assuring money and effort is well spent
  - The three legs of Administrative Simplification
  - Where to begin?
- Identifying “chunks”
- What is “reasonable?”
- Who will do the work?

Experiential Based

- Rural Hospital Experiences – Best Practices
- Community Hospitals: Security Needs
- Large Health Systems:compliance tracking tools
- How to establish priorities
- Determining “Chunks”

LESSONS LEARNED

#1

EDI Remains a Major Concern

- Vendor Readiness
- Facility Readiness

RECOMMENDATION

#1

EDI Task force working with vendors and health plans to identify data elements and prepare for testing by April 14, 2003

LESSONS LEARNED

#2

Most of HIPAA Compliance comes down to Behavioral Changes

Staff….Physicians….volunteers…etc

RECOMMENDATION

#2

Staff Training

✓ Ongoing

✓ Focused

LESSONS LEARNED

#3

Future Compliance demands solid

- ✓Policies
- ✓ Procedures
- ✓ Training

RECOMMENDATION

#3

Establish a "HIPAA Coordinators" Group to Encourage Exchange of Information

LESSONS LEARNED

#4

Need to consider

"Contingency Plans"

RECOMMENDATION

#4

Get Moving

Get Serious

Get Done

Protecting PHI

- The end goal: find it, follow it and protect it
  - All the activities basically follow the PHI
  - More than electronic, paper and oral
  - What is it and who controls it?
    - Surprise: not you
    - It's everything for all intents and purposes!

Some days we just get stuck, and bogged down.
Some days all you can do is smile and wait for someone to kindly remove your butt from the hole you find it wedged into.

Common Security Compliance Findings

Applicable to Community Hospitals and all Other HIPAA entities (that's the lesson learned!)

The Proposed HIPAA Security Standards: Subject Areas

- Administrative Procedures [45 CFR §142.308(a)]
- Physical Safeguards [45 CFR §142.308(b)]
- Technical Security Services [45 CFR §142.308(c)]
- Technical Security Mechanisms [45 CFR §142.308(d)]

Administrative Procedures

- Certification Process and Program Development [45 CFR §142.308(a)(1)]
  - Internal or external
- Contingency Program Development [45 CFR §142.308(a)(3)]
  - Must include: Applications and Data Criticality Analysis
  - Data Backup Plan
  - Disaster Recovery Plan for the Entire Enterprise
  - Emergency Mode of Operation
  - Testing and Revision Procedures

Administrative Procedures (continued)

- Records Processing Policies and Procedures Development [45 CFR §142.308(a)(4)]
  - Receipt, manipulation, storage, dissemination, transmission, disposal of PHI
- Information Access Control Policies and Procedures [45 CFR §142.308(a)(5)]
  - Access Authorization (overall access procedures)
  - Access Establishment (Initial right of access)
  - Access Modification (job change or termination)

Administrative Procedures (continued)

- Security Configuration Management Policies [45 CFR §142.308(a)(8)]
  - Hardware and software installation and maintenance review and testing
  - Hardware and software inventory
  - Security Testing (host and network component penetration testing) Protocols and Services

Administrative Procedures (continued)

- Training Program Development [45 CFR §142.308(a)(12)]
  - Security Awareness Training for ALL Personnel
  - Periodic Reminders
  - Virus Protection Education
  - Log in Access Education
  - Password Management Education

Physical Safeguards

- Assigned Security Responsibility [45 CFR §142.308(b)(1)] (must understand all aspects of information security)

Technical Security Systems

- Access Control [45 CFR §142.308(c)(1)(i)]
  - Implementation Features - at least one of the following:
    - Context-based
    - Role-based
    - User-based
- Audit controls [45 CFR 42.308(c)(1)(ii)]
  - Mechanisms to record and examine system activity

Technical Security Mechanisms

- Network Controls [45 CFR §142.308(d)(2)]
  - Alarm (IDS)

"The computer expert is here, Mr. Rumson."

Do Not Delay

LARGE IDS

- Multiple Acute Care Hospitals
- Long-term Care Facilities
- Health Plan
- Clinics
- Dental Clinics
- Faculty Practice Plans

HIPAA Implementation Situation

- Organize HIPAA implementation for a large, urban single entity healthcare system with 130 facilities ranging from large acute care to small clinics.
- Track and monitor implementation progress throughout a diverse, distributed entity.

HIPAA Implementation Tasks

- Create an implementation plan for 7,500 HIPAA recommendations and findings.
- Organize and coordinate central and local implementation teams.
- Manage and track compliance implementation as findings are addressed in an auditable manner.

HIPAA Implementation Plan

- Perform Analysis
- Design Implementation Projects
- Formulate Organization Structure & Operating Processes
- Formulate Organizational Roles and Responsibilities
- Create and Deploy Implementation Tools

Analysis

- Recommendations and findings were extracted from reports and categorized with 25 unique identifiers that include regulation paragraph number and section, implementation workgroup, and action required for implementation.

Projects

- Projects were formulated based on type of action required on recommendations and findings.
- Projects were prioritized based on the regulatory risk profile of the entity.

Organization

- Structure was designed to include executive management, privacy officer, compliance directors, implementation workgroups and consultant subject matter experts.
- Process for organizational behavior was pre-defined to ease information and workflow during implementation.
- Roles & responsibilities were defined within process to assist team behavior and function.

Tools

- Compliance tracking database was design and developed to house recommendations, work groups and projects.
- Tool enables users to monitor their area of responsibility for HIPAA implementation.
- Tool provides compliance audit trail for regulatory enforcement inquiries.

Compliance Tracking Tool

- Features:
  - My Dashboard, for executive level compliance tracking
  - My Recommendations, for manager level tracking of activity by recommendation and finding
  - Projects, for project creation, maintenance and tracking
  - Recommendations, for user designed query searches of recommendation database, and recommendation management.

Compliance Tracking Tool

My Dashboard

My Statistics

Recommendation Statistics | Recommendation Search

Recommendations by Reg. Class Level 2

Name	Rec.	Prj.
Access of Individuals to their own PHI	318	314
Accounting Of Disclosures	152	152
Additional Requirements for Health Plans	0	0
Additional Restrictions on Uses and Disclosures Requested by Individuals	24	24
Administrative Procedures	1298	1298
Alternative Means or Location of Communication Requested by Individuals	48	48
Amendment of PHI	80	80
Code Sets	0	0
Complaints to the Covered Entity	0	0
Coordination of Benefits	33	0
Electronic Signature Standards	0	0
Eligibility for a Health Plan	53	53
Enrollment & Disenrollment in a Health Plan	0	0
General Provisions	0	0
Group Health Plan	6	2
Health Care Claim Status	34	34
Health Care Claims or Equivalent Encounter Information	0	0
Health Care Payment and Remittance Advice	34	34
Health Plan Premium Payments	0	0
Mitigation of Harmful Effects of a use or disclosure	1	1
Notice of Privacy Practices	0	0
Physical Safeguards	466	466

Recommendations by Project Priority

Name	Rec.	Prj.
High	126	4
Low	3	4
Medium	99	2
Mission Critical	0	1
None	0	0

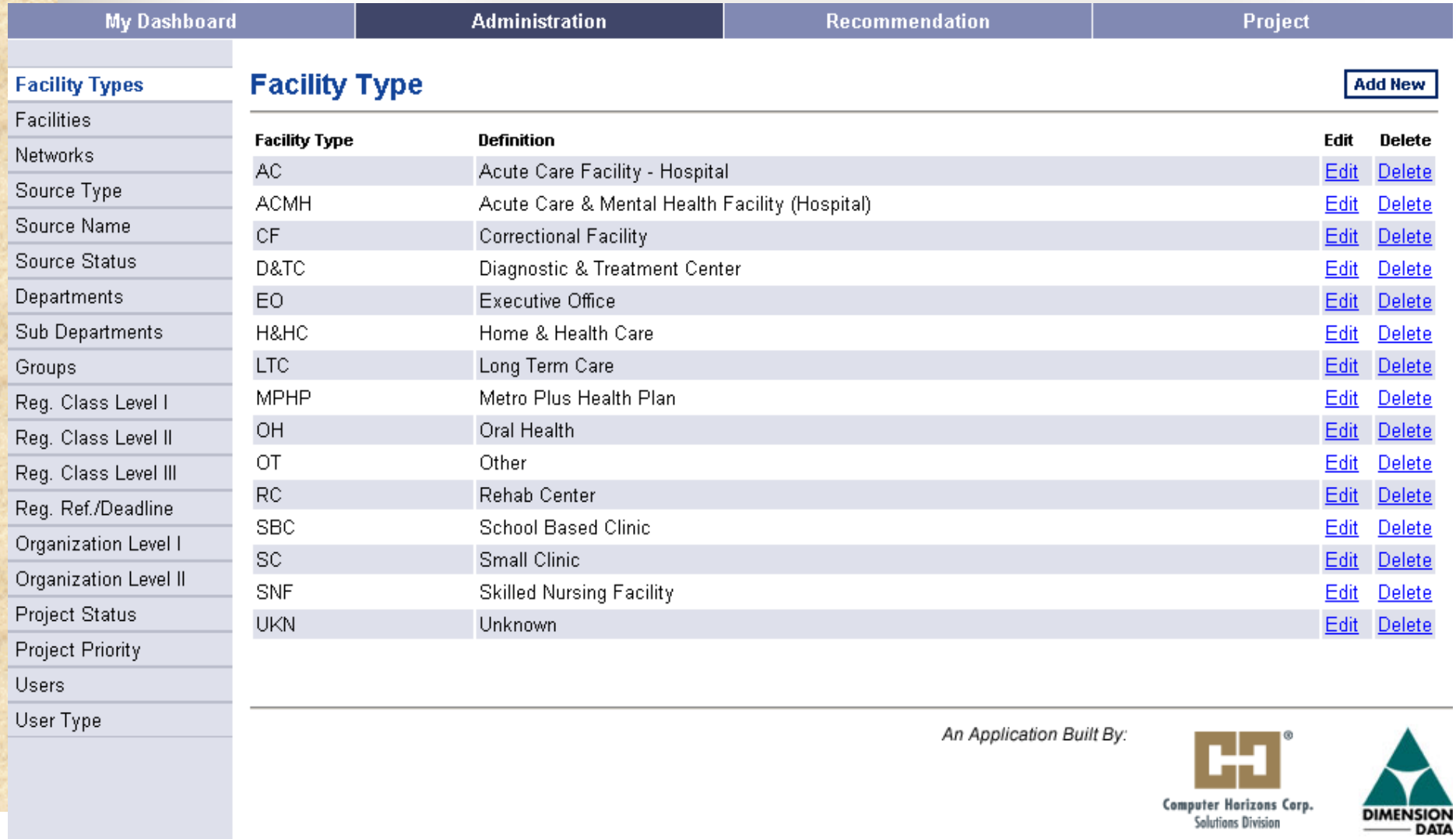
Recommendations by Project Status

Name	Rec.	Prj.
Completed	0	0
Defined	0	0
In Progress	0	0
Plan Complete	228	11
Recommendations assigned	0	0
Started	0	0
Stopped before completion	0	0
Workgroup assigned	0	0

Recommendations by Status

Name	Rec.	Prj.
Assigned to group	0	0
Assigned to project	6855	6747
Compliance in progress	0	0

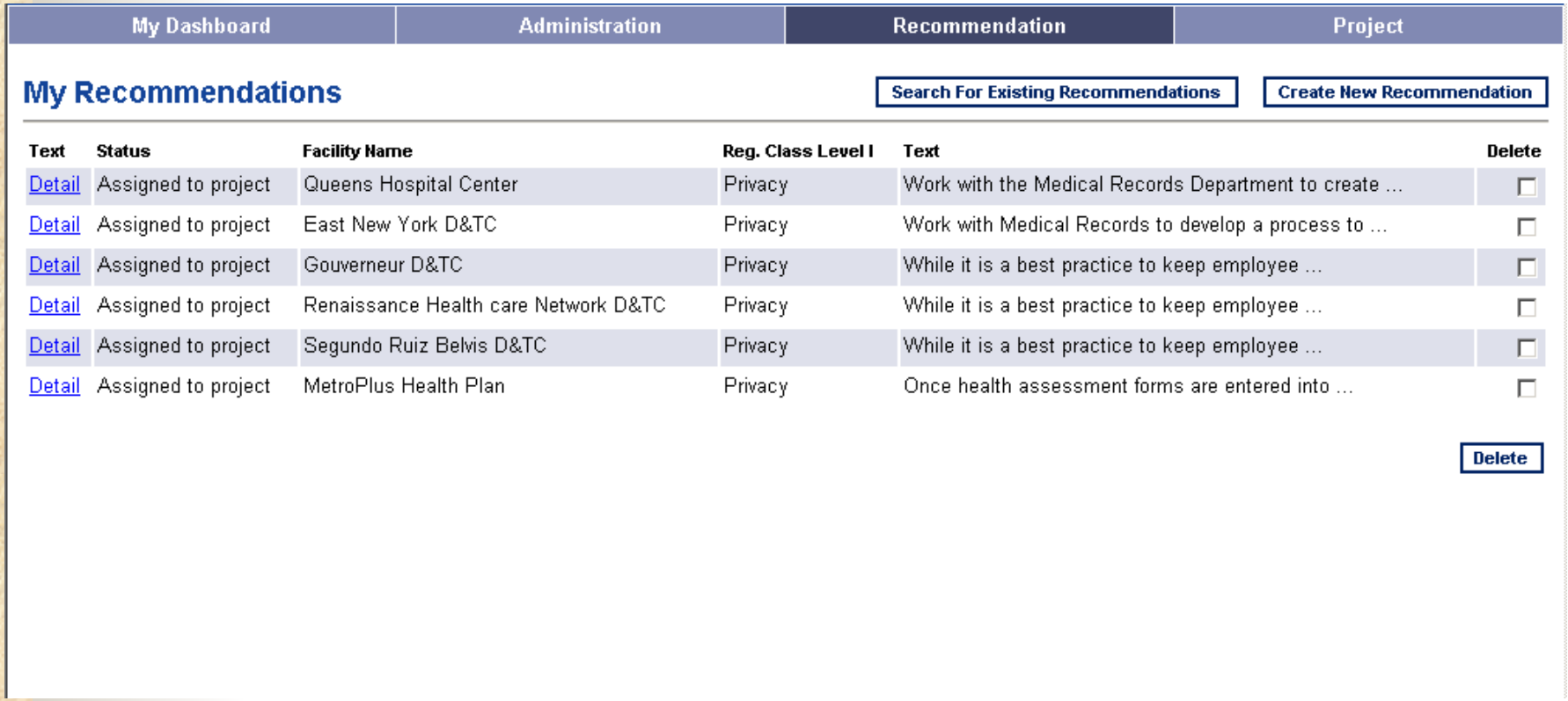
Compliance Tracking Tool



CHC Healthcare Solutions

HIPAA PROS.com

Compliance Tracking Tool



My Dashboard | Administration | Recommendation | Project

My Recommendations

Search For Existing Recommendations | Create New Recommendation

Text	Status	Facility Name	Reg. Class Level I	Text	Delete
Detail	Assigned to project	Queens Hospital Center	Privacy	Work with the Medical Records Department to create ...	☐
Detail	Assigned to project	East New York D&TC	Privacy	Work with Medical Records to develop a process to ...	☐
Detail	Assigned to project	Gouverneur D&TC	Privacy	While it is a best practice to keep employee ...	☐
Detail	Assigned to project	Renaissance Health care Network D&TC	Privacy	While it is a best practice to keep employee ...	☐
Detail	Assigned to project	Segundo Ruiz Belvis D&TC	Privacy	While it is a best practice to keep employee ...	☐
Detail	Assigned to project	MetroPlus Health Plan	Privacy	Once health assessment forms are entered into ...	☐

Delete

Compliance Tracking Tool

My Dashboard | Administration | Recommendation | Project

Recommendation Detail:

Back to Main Page

Description

Edit

Text

Work with the Medical Records Department to create a procedure to ensure that the records are included in the designated record set.

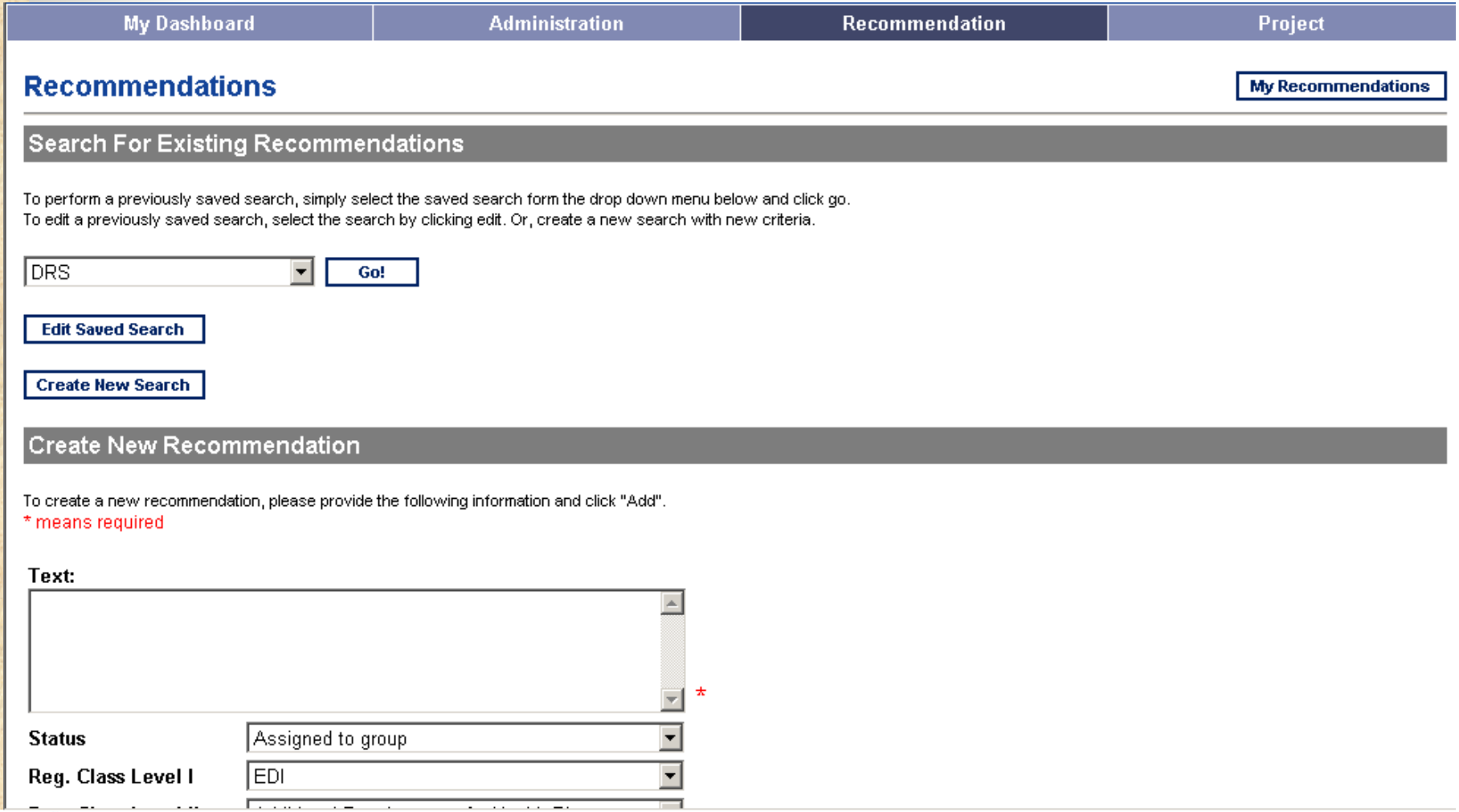
Status	Assigned to project
Reg. Class Level I	Privacy
Reg. Class Level II	Access of Individuals to their own PHI
Reg. Class Level III	N/A
Regulatory Reference	164.524
Regulatory Deadline	2003/04/14
Org. Level I	Local Type 2
Org. Level II	Designated Record Set
Facility Name	Queens Hospital Center
Facility Type	AC
Dept Name	Psychiatry
Sub Dept Name	N/A
Network Name	Queens Health Network
Network Code	QN
Location	70
Source Name	Queens Hospital Center
Source Section	Behavioral Health/Psychiatry
Source SubSection	

Notes

Add

Notes	User	Date

Compliance Tracking Tool



Compliance Tracking Tool

My Dashboard | Administration | Recommendation | Project

Projects

Detail	Project Name	Manager	Sponsor	Start Date	End Date	Priority	Status
Detail	AO – Correctional Health					N/A	N/A
Detail	AO – Group Health Plan					N/A	N/A
Detail	AO – Health & Home Care					N/A	N/A
Detail	AO – Metro Plus					N/A	N/A
Detail	CO – Business Associates			2002/06/01	2004/04/14	N/A	N/A
Detail	CO – Chain of Trust Partners					N/A	N/A
Detail	CO – Trading Partner Agreements					N/A	N/A
Detail	DRS – Access of Individuals to their own PHI			2002/10/01		N/A	N/A
Detail	DRS – Accounting of Disclosures			2002/10/01		N/A	N/A
Detail	DRS – Additional Restrictions on Uses & Disclosures by Individuals			2002/10/01		N/A	N/A
Detail	DRS – Amendment of PHI			2002/10/01		N/A	N/A
Detail	DRS – Safeguards (administrative, technical and physical)			2002/10/01		N/A	N/A
Detail	DRS – Uses & Disclosures for TPO			2002/10/01		N/A	N/A
Detail	DRS – Uses & Disclosures of PHI: General Rules			2002/10/01		N/A	N/A
Detail	DRS – Uses & Disclosures: Authorization or Individual Agree or Object NOT REQUIRED			2002/10/01		N/A	N/A
Detail	DRS – Uses & Disclosures: Authorization REQUIRED			2002/10/01		N/A	N/A
Detail	DRS – Uses & Disclosures: Individual Agree or Object REQUIRED			2002/10/01		N/A	N/A
Detail	EDI – Additional Requirements for Health Plans			2002/10/01		Low	Plan Complet

Compliance Tracking Tool

My Dashboard | Administration | Recommendation | Project

Project Details:

Back | Delete

Project Description

Edit

Name: CO – Business Associates
Manager:
Sponsor:
Start Date: 2002/06/01
End Date: 2004/04/14
Priority: N/A
Status: N/A
Description:

Notes

Add

Notes	User	Date

Recommendations

Detail	Recommendation Text	Status	Delete
Detail	A procedure should be developed for all vendors requiring them to submit invoices for payment without the PHI, if the PHI is not necessary for the order.	Assigned to project	☐
Detail	A procedure should be developed specifically for Quest Diagnostics indicating that invoices should be submitted for payment without the PHI, if the PHI is not necessary for the order.	Assigned to project	☐
Detail	To the extent that some vendors receive personally identifiable health information from Bellevue for reasons other than treatment (Quest is involved in patient treatment), and that reason is …	Assigned to project	☐
Detail	A procedure should be developed specifically for Quest Diagnostics, and for any other vendors that include PHI on invoices. Such a procedure would require the originating Department to review the …	Assigned to project	☐
Detail	To the extent that some vendors receive PHI from CIH for reasons other than treatment, payment or health care operations (Quest is involved in patient treatment), and such vendors are providing …	Assigned to project	☐
Detail	A procedure should be developed specifically for any other vendors that include PHI on invoices. Such a procedure would require the originating Department to review the invoices and submit it for …	Assigned to project	☐

Summary

- Use of an implementation partner has distinct advantages to the organization:
  - Available implementation tools.
  - Proven HIPAA implementation management methods and techniques.
  - Regulatory subject matter expertise built through training and experience.

Where to start?

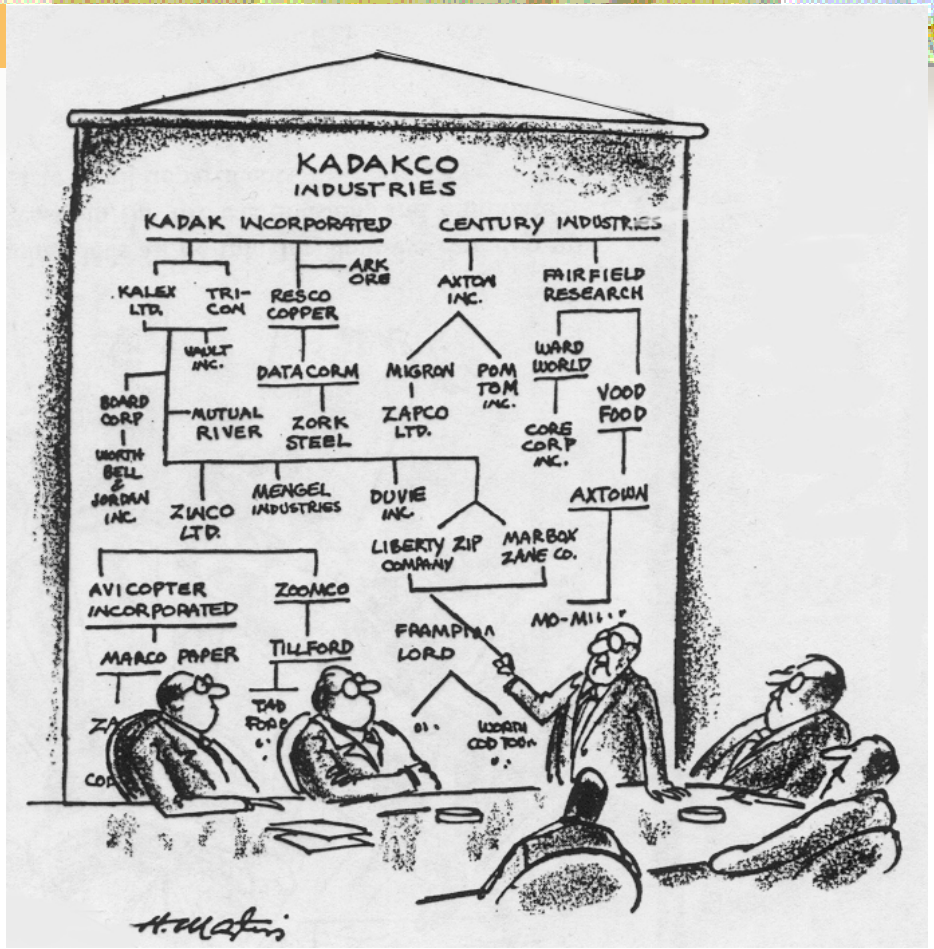
- Assuming a work plan exists from the initial baseline assessment, it is clear that providers must first address “HIGH” risk areas
- “Typical” high risk areas include:
  - Vendor readiness
  - Health Plan directives
  - Lack of Compliance Plan components (required)
  - Training, training and more training
  - Business Associates
  - Physical Security
  - Records management

Setting Priorities

- Infrastructure issues
  - Firewalls
  - Protecting the network
  - Access controls
- Patient rights
  - HIPAA is a patient-centric set of regulations and the patient rights (Notice of Privacy Practices, handling disclosures) documentation of decisions is a critical step

Manageable "Chunks"

- Working in the above priorities, define chunks of tasks that can be delegated to the work groups all designed to address the high priority areas
  - Security in the systems: effected by decisions already made to address the EDI concerns
  - EDI task forces: focus is on meeting testing parameters and assuring the system (whether computerized or manual) allows all components of your HIPAA Covered Entity to capture the required data elements
  - Privacy projects: awareness training, formation of compliance office, documents, management of patient rights and Business Associates



"And now, let's determine if we are a covered entity, affiliated single covered entity, hybrid covered entity or organized health care arrangement."

Covered Entity Decisions

- Single entity
- Affiliated Single entity
- Hybrid entity
- Organized health care arrangement
  - Considerations
  - Pros/Cons
  - documentation

Improving Cash Flow

- EDI standards require uniform

  codes for all payers
- Uniformity = Cost Savings
- This is the bottom line!

Question & Answer

Contacts

- Janet Himmelreich
  - 215.517.4920
  - janet_himmelreich@computerhorizons.com
- John Whitman
  - 215.517.4985
  - john_whitman@computerhorizons.com
- Martin Rogers
  - 703.927.4205
  - martin_rogers@computerhorizons.com
- Melissa Campbell
  - melissac@chcsolutions.net