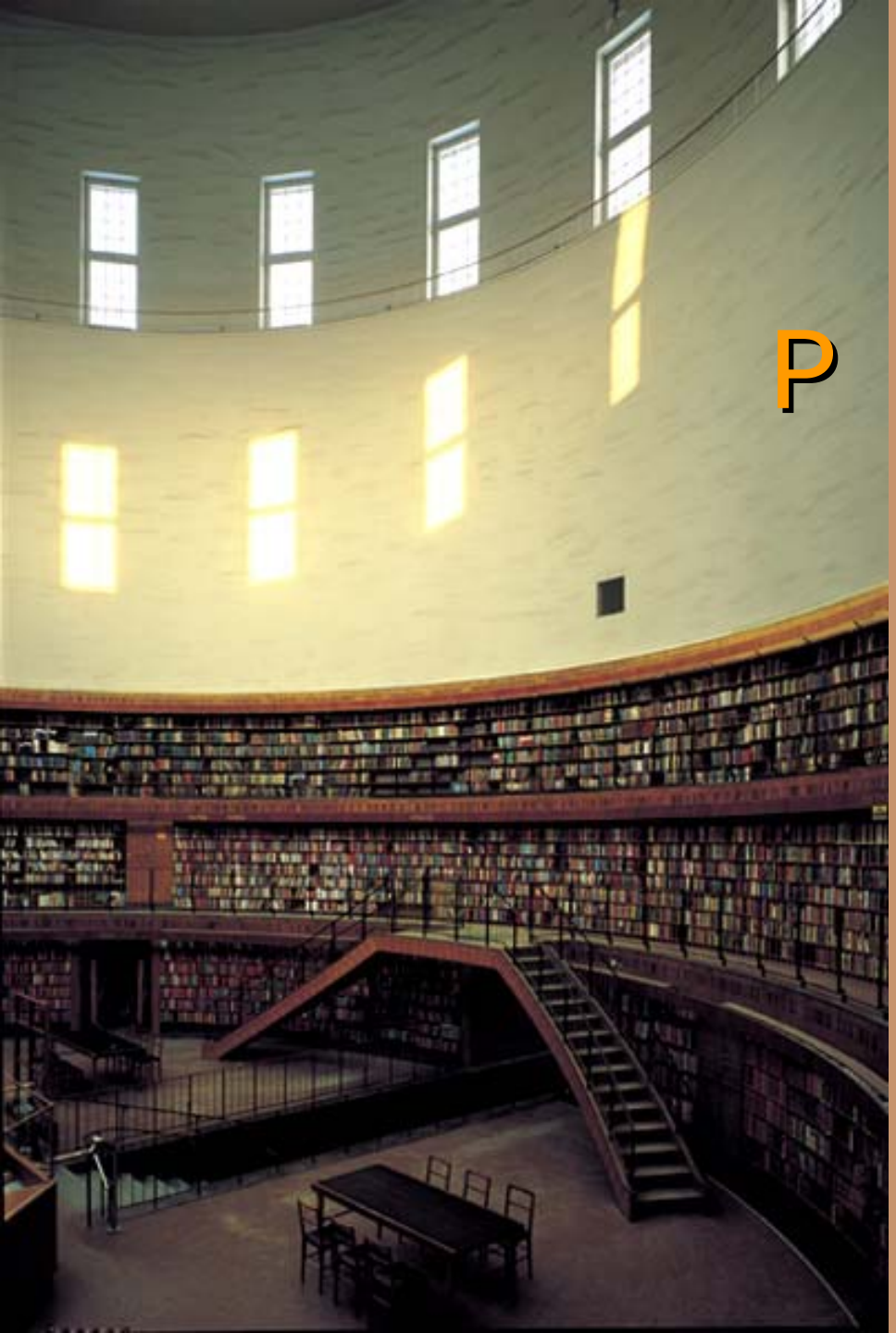


P w C

# *HIPAA Assessment and Implementation*

*Presented to the*
*Fifth HIPAA Summit*
*October 30, 2002*

# The P w C Approach

- Guiding Principles
- Assessment Process
- Implementation Projects
- Considerations for Privacy Implementation

# The P w C Approach

## Guiding Principles for Privacy

- HIPAA solutions should support business objectives, not jeopardize them
- Prioritize among new processes and increased requirements – HIPAA compliance requires reasonable, good-faith efforts
- No one meets HIPAA privacy requirements now – it makes sense to focus assessment efforts on needed processes
- Organize efforts around specific projects to establish focus – prioritize, sequence, integrate and manage resources
- IT solutions may play a role in supporting privacy processes

# The P w C Approach

## Guiding Principles for Security

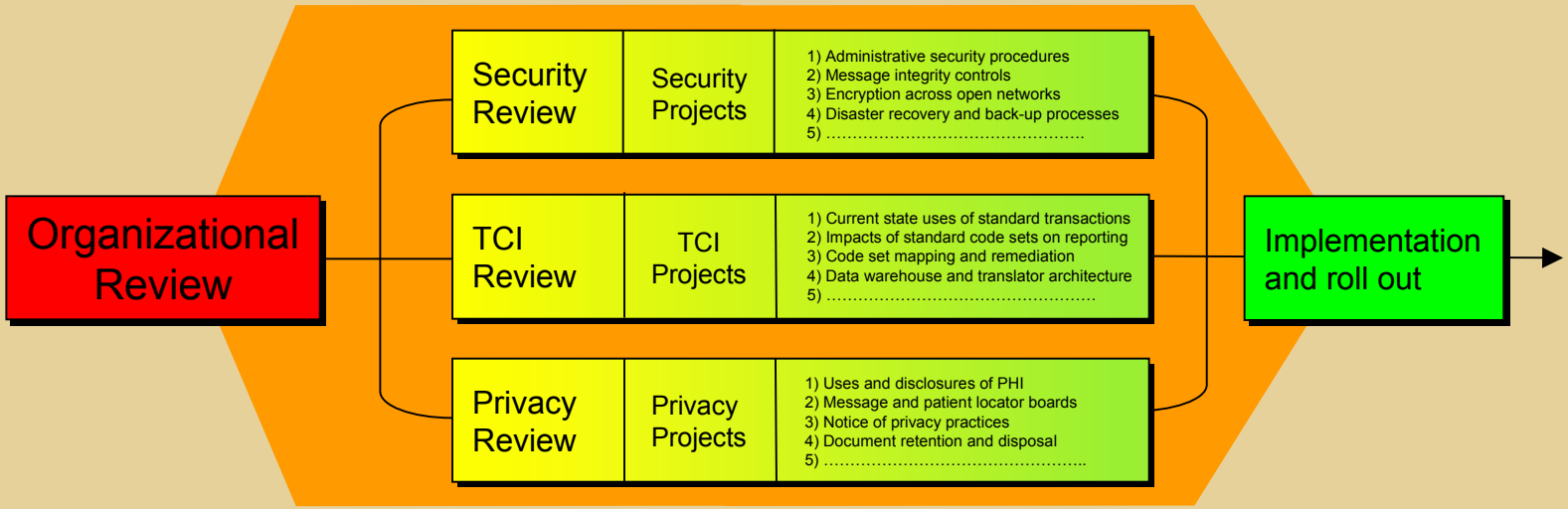
- Few cutting edge or groundbreaking requirements – most represent best practices already current in other industries
- Many HIPAA security practices already reflected in current programs – benefit of Y2K
- Gap analysis approach makes sense to identify areas for improvement
- Organize efforts around specific projects to establish focus – prioritize, sequence, integrate and manage resources
- Many aspects, especially physical security, work hand in hand with privacy – operational focus

# The P w C Approach

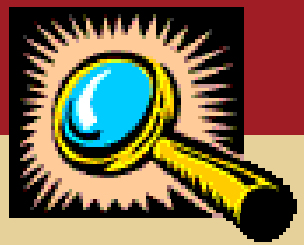
## Guiding Principles for Transactions

- HIPAA solutions should support business objectives, not jeopardize them
- Take advantage of time available through one-year extension of deadline
- Some systems may not need much work to meet HIPAA transaction requirements, while others will need major modifications
- Four basic approaches:
  - Modify or upgrade your system
  - Employ an add-on
  - Replace your system

# HIPAA Assessment Process



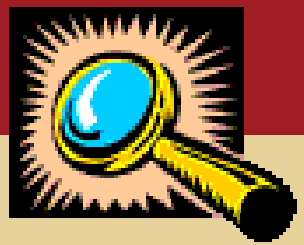
# Organizational Review



## Structure, Strategy and Relationships

- Determine HIPAA status of each legal entity as covered entity or business associate
- Organize HIPAA project structure – steering committee, manager, task group members
- Evaluate personnel and training policies and procedures
- Review structure of employee health benefit plans
- Review relationships with key business associates
- Review corporate initiatives potentially affected by HIPAA
- Produce high-level assessment and solution development work plan

# Privacy Review



## Privacy Readiness Assessment

- Document internal and external flows and uses of PHI – written, spoken, faxed, electronic; identify risk points
- Evaluate existing privacy and physical security practices
- Review confidentiality and retention policies and procedures
- Establish privacy program elements – privacy official, written policies and procedures
- Produce *pro forma* privacy gap analysis
- Link findings to implementation projects
- Develop high-level project work plans and budget estimates

# Privacy Projects

- Specific project templates defined for privacy
- Adapted and customized for client characteristics
- Define project, summarize regulations, key project decisions and guidelines, key work plan elements, potential IT-based solutions
- PwC and client staff refine application to client organization through review findings, focus groups, brain-storming
- Identify and rank possible solutions and approaches, choose best fit solution
- Produce refined implementation plan, staffing budgets and documentation

# Privacy Projects

1. Access, Inspection and Copying of Protected Health Information
2. Accounting for Disclosures of Protected Health Information
3. Alternative Communication of Protected Health Information
4. Amendment of Protected Health Information
5. Authorization, Consents and Opportunities to Object
6. Business Associate Provisions and Agreements
7. Confidentiality Policy Review and Revision
8. De-Identification of Protected Health Information
9. Disclosure of Protected Health Information by Fax Machine or Printer
10. Disclosure of Protected Health Information by Telephone
11. Documentation of Privacy Policies and Procedures
12. Human Resources Policies Review and Revision
13. Role-Based Access Review and Update
14. Entity Relationships and Agreements
15. Minimum Necessary Disclosure Policy and Determination Protocols
16. Mitigation of Deleterious Effects of Improper Uses and Disclosures
17. Notice of Information Practices
18. Privacy Program and Privacy Official
19. Process for Responding to Legal and Law Enforcement Requests
20. Receiving and Handling Privacy Complaints (External and Internal)
21. Records Retention, Storage and Disposal Policies Review and Revision
22. Restriction of Further Disclosure of Protected Health Information
23. Revision of ERISA Plan Document Disclosures
24. Staff Training in Privacy Policies and Security Awareness
25. Use of Protected Health Information at Home or Off-Site
26. Use of Protected Health Information for Marketing and Fund-Raising Purposes
27. Uses and Disclosures of Protected Health Information
28. Verification of Identity for Non-Routine Requests for Use and Disclosure
29. Personal Representatives and Individuals' Control of Health Information
30. Categorization of Uses and Disclosures and Designation of Record Sets
31. Patient Directory Information
32. Physical Security
33. Research Programs
34. Stakeholder Awareness Campaign
35. State Regulatory Guidance

# Security Review

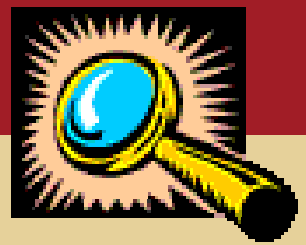
## Security Readiness Assessment

- Review system documentation to understand IT environment
- Interview security and network staff
- Review security policies and procedures
- Identify needed modifications and additions to existing security P&Ps
- Perform technical security diagnostic reviews on key platforms
- Develop *pro forma* security needs assessment linking regulations to current state of security program and recommended projects
- Document security risks associated with transmission, dissemination, usage and storage of PHI
- Develop high-level project work plans and budget estimates

# Security Projects

- Enterprise Security Architecture/Information Security Management
- Risk Management/Business Continuity Planning
- Secure Configuration Management
- Business Associate/Chain of Trust Agreements
- Processing Records and Media Controls
- Personnel Procedures
- Auditing
- Information Security Policy& Security Awareness Training
- Physical Security/Workstation Security

# Transaction & Code Set Review



## Transaction & Code Set Readiness Assessment

- Assess system architecture and infrastructure
- Evaluate EDI interfaces and data storage environment
- Evaluate transaction systems, clearinghouse relationships and translator capabilities
- Review work processes supported by transaction and reporting systems
- Review implementation and maintenance of code sets and identifiers
- Identify all applicable code sets and supporting code set uses.
- Develop integrated map of systems environment, preliminary information flows, and relevant technology initiatives

# Transaction & Code Set Projects

- Transaction & code set remediation project management
- Upgrade current EDI infrastructure
- Translator evaluation and implementation
- Identify, select, and implement HIPAA data store
- Analysis and Implementation of vendor system solution
- Develop and certify key trading partner exchanges
- Quality assurance and testing
- Code set remediation
- Identifier modifications

# Considerations for Privacy Implementation

P w C

# Records Retention Program

- Why is an effective records retention program so important?
  - Helps locate records in Designated Record Sets (DRS) and fulfill requirements
  - Conscientious administration decreases overall liability
- Should address retention periods, storage standards, disposition
- Identify, map and locate records in DRS
- Identify relevant statutory and contractual retention limits, determine highest common denominators
- Incorporate physical security principles – secure storage, controlled access
- Specify standards for culling and disposal of outdated records

# Access Requirement

- Pertains to records in (DRS) for as long as records are maintained
- DRS may include records in multiple covered entity locations, on-line/off-line, on-site/off-site, different media and in possession of business associates
- Access options – how much will people want to see?
- If you build it, they will come…?
- Timeframe: 30 days for in-house records, one 30-day extension permitted for off-site records
- Delivery issues:
  - Formatting and presentation of electronic documents
  - On-site review may be impractical in regional settings
  - Provision of access on-line or by mail

# Amendment

- Amend within 60 days; one 30 day extension permitted
- Logistics of locating incorrect record
- Amendment of paper records
  - Amend with addendum, statement of disagreement and/or rebuttal
- Amendment of electronic records
  - Electronic link between original incorrect record and amendment; does file structure permit “attachment” or link?
  - Process correcting transaction (e.g., claim or enrollment)
  - Statement of disagreement and rebuttal?
  - Render record into physical form, treat as paper

# Accounting Requirement

- Applies to all disclosures after 4/14/2003, except those made for:
  - Treatment, payment or healthcare operations
  - Regulatory agencies and legal processes
  - With individual's authorization
- How does one report on disclosures for up to six years prior to request?
- Record disclosures as they are made or search at time of request?
- Disclosure database:
  - Track required elements for reporting
  - Track requests for accounting
  - Index by individual name or identifier

# Minimum Necessary

- Applies both to uses and disclosures
- Standards for *disclosures* are straightforward:
  - Protocols for routine or recurring disclosures
  - Process for determining minimum necessary in other cases
- Standards for *uses* are less clear – make reasonable efforts to limit uses to minimum necessary
- Implementation strategies:
  - De-identification of reports, databases, reporting files
  - Role-based access :: job function :: job description
  - Field-level access controls
  - Review and modify commonly used forms and system screens

# Documentation

- Maintain written policies and procedures that demonstrate how the covered entity achieves compliance
- If it isn't documented, it doesn't exist!
- Document the decisions made in implementation, even if decision is to take no action
- P&Ps should describe process, designate responsible staff, specify time frames
- Retention requirements for medical and business records set by state law, contracts or program requirements
- Retention of records required by HIPAA (e.g. privacy notice, requests for access, authorizations) is six years

# Identity Verification

- Verify identity and authority of persons requesting PHI who are not known to the covered entity
- *Identity* established by personal information elements:
  - **Weaker semi-private elements:** DOB, SSN, mother's maiden name, current mailing address, date of last claim or visit
  - **Stronger private elements:** prom date, color of first car, favorite Beatles song
- Best information elements are experiential, based in long-term memory
- Strength of information already available vs. cost of populating with stronger information
- *Authority* established by legal basis:

# Physical Security

- Placement of fax machines and printers, document pickup, sharing between functions
- Access controls – locking or monitored doors, positioning of PHI records and computer monitors in relation to customer areas
- Secure storage of physical documents and computer media with PHI – lockable storage area or file cabinets (not in cardboard boxes under desks!)
- PHI document disposal – trash vs. recycling vs. shredding
- Work in progress placed in locking drawer during non-business hours
- Positioning of interview areas in relation to waiting area

# Business Associates

- Vendor receives PHI from covered entity (CE), performs service using PHI
- CE must have business associate (BA) agreement with vendor
- BA agreement provisions should reflect degree of risk delegated to BA
- Basic BA agreement – use for relationships with access to PHI or non-complex low-risk services
- Enhanced BA agreement – use in significant risk relationships, e.g. health plan/TPA, provider/clearinghouse
- Provisions for consideration:
  - Detailed specifications of permitted uses and disclosures (parties should negotiate)
  - Indemnification of CE in all derivative agreements
  - Approval of subcontractors

# Employee Health Benefit Plans

- Typically includes health, dental, vision, Rx, behavioral health, some EAPs
- EHBP is covered entity, not employer or plan sponsor
- Characterize some covered functions as activities of plan sponsor?
- Modification of plan documents enables use of limited PHI
- Some EHBPs can do limited privacy implementation – §164.530(k)
  - Benefits provided through insurance contracts
  - Do not create or receive PHI
- Separation of EHBP and HR functions – physical, personnel, P&Ps, employee benefit/personnel files
- Define DRS for EHBP vs. information in employment records
- Assess uses of PHI from disease/case/absence management, return to work, integrated disability programs

# Alternative Communications

- Grant requests for communications of PHI to alternate locations or by alternate means
  - Providers – if request is reasonable
  - Health plans – if disclosure would endanger individual
- Alternate locations – e.g. office/relative/PO box instead of home
- Alternate means – e.g. fax/phone/e-mail instead of postal mail
- Re-route or suppress printing of system-generated documents
- Outgoing communications containing PHI, e.g. appt reminders, test results, EOBs, authorizations/referrals, balance bills
- Notify staff of alternative communication request in effect
- Area of potentially significant civil liability

# Workforce Training

- Training in the covered entity's privacy policies and procedures
- Curriculum options: general CE policies, focused training on specific processes; HIPAA awareness?
- Practical delivery options:
  - Individual printed training or policy manuals
  - CBT – CD-ROM, intranet or web-based, learning management system, electronic document libraries connected by hyperlinks
- Staff targeting options: clinical, administrative, management, job class
- Document completion of training – certificate, sign-in log, LMS tracking
- Other parties to include:
  - Medical staff (hospitals), contracted providers (health plans)
  - Volunteers, students, contractors, temporary/registry personnel?

# Mitigation

- Mitigate harmful effects of violations of privacy policies or regulations
- Awareness through monitoring
  - Compliance program hotline
  - Specific incidents or patterns of customer or business associate complaints
  - Periodic internal compliance audits
- Mitigation through action
  - Determine nature and extent of disclosure, feasibility of recovery
  - Review with response team (operations, compliance, risk management, legal)
  - Determine need to notify affected individual, federal authorities
  - Document incident and actions taken
  - Intervention/sanctions with staff or business associates
- Encourage responsible and open communication; avoid cover-ups

# Compliance and Risk Mgmt

- Major risk areas – regulatory, reputational, civil liability
- Enforcement by DHHS – OCR (privacy) and CMS (transactions)
  - OCR has ~ 200 staff (e.g. four per state)
  - Technical assistance in first year, reactive thereafter?
- Assume ~ 2M covered entities? Physicians, dentists, hospitals, ancillary providers, licensed health plans, employer health plans…
- Likely to focus on flagrant violators – big names, deep pockets
- Trial attorneys' view:
  - HIPAA does not create private right of action
  - File civil suit in state court for privacy violations
  - Individual or class action suits alleging negligence
  - Failure of covered entity to comply with federal "standard of care"
- Anticipate explaining decisions and processes to a third party

# Questions and Discussion

*For more information, contact:*

Rhys W. Jones, MPH
National Director, HIPAA Privacy Services
(813) 222-6237 • rhys.w.jones@us.pwcglobal.com

P w C