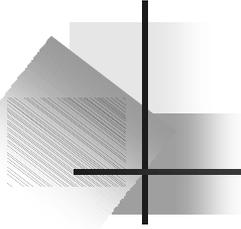


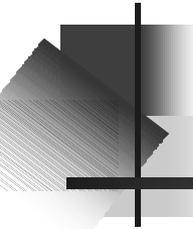
Business Operations, Security, and Privacy

*Considerations in Designing a
HIPAA-Compliant Information
System*

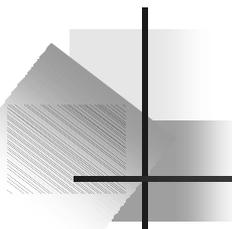


This Section Covers:

- Standards Integration Overview
- Business Processes
- Medicare/Private Payers
- TCS Technology-related Considerations
- Privacy Considerations
- Security Technology-related Considerations
- When Shopping for a Vendor

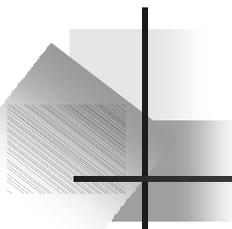


Standards Integration Overview



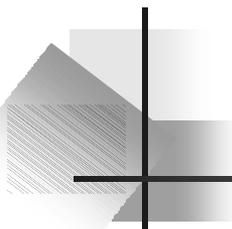
HIPAA and the Industry standards for an EHR/EMR

- Privacy – standard for oral, written, electronic communications
- Security – standard for infrastructure, storage, transmission
- TCS – electronic content for billing
- Confidentiality laws
- Functionality
- Electronic standards
 - Terminology
 - Diagnosis
 - Procedure
 - Lab
 - Messaging



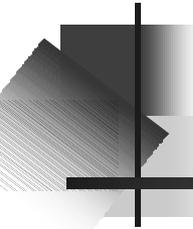
HIPAA and ADP

- To help bring providers into compliance
- To help move the state forward into an electronic environment
- To help institute standards for better health care for the citizens of California

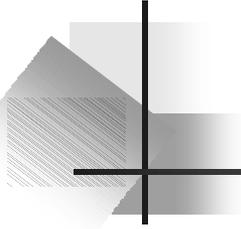


Why are we here today?

- To talk about the right questions to ask about
 - Your organization
 - Your business processes
 - Compliance with ADP's requirements in the context of HIPAA
 - When shopping for technology solutions

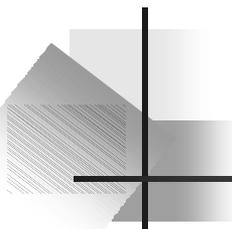


Business Processes



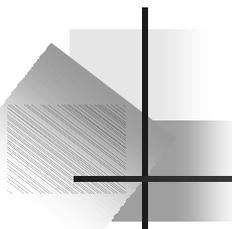
Examine Current Billing Process

- What are your billing needs
 - How many different insurance companies do you bill
 - How many government programs do you bill
 - How many claim resubmissions
- Explore whether a single billing system can meet the needs for multiple payers



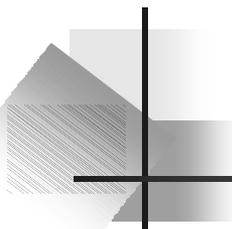
Examine Current Billing Process

- Review existing workflows for the 837 transaction
 - Can workflow be improved/automated?
 - Can information returned be better utilized/automated?
 - Do you use non-standard codes in these processes?
 - Can you incorporate standard codes or do you need to crosswalk?
 - Is there value in implementing HIPAA transactions which you don't currently conduct electronically?
 - Is there value in implementing transactions not currently required by HIPAA?



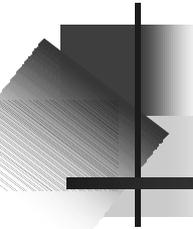
Examine Current Billing Process

- Have you made changes to your business processes to streamline and reduce costs?
- How can you take advantage of HIPAA?
Example...
 - Eligibility Verification
 - Check each time
 - Build internal database
 - Real time versus batch mode (daily appointment schedule or as patients arrive?)

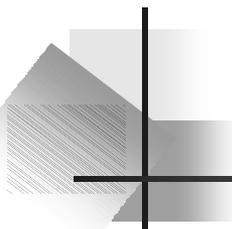


Changes to Payer Systems

- Major changes in all payers' direct data entry systems
- Data content (data elements) must meet the data content portion of the national electronic standard
- Systems will also need to be capable of receiving data transfers (directly or through a clearinghouse) from providers
- If provider chooses to send data electronically, payer must accept

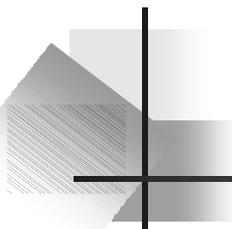


Medicare/Private Payers



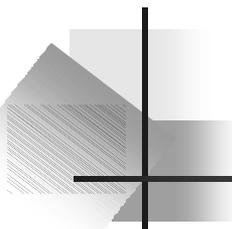
Medicare

- Major changes on current direct data entry system
- ***Standardized Trading partner agreement*** coming up
- Companion document establishing Medicare-required situational data elements
- Free/low cost HIPAA-compliant software available from carriers and fiscal intermediaries for providers to submit Medicare claims electronically
 - Free PC-print software for electronic Medicare remittance advice (835) transactions
 - <http://www.cms.gov/providers/edi>



Medicare

- Medicare software allows providers to create a HIPAA-compliant claim. Cannot be used for other payers.
- For other HIPAA transactions, providers are expected to obtain own software
- Clearinghouses offer an alternative

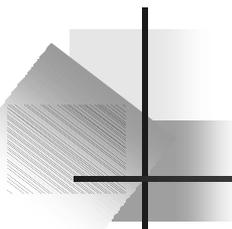


Private Payers

- Updating web sites to allow interactive transactions
- Developing “companion documents” to define requirements for the situational data elements
- Providing trading partner agreements

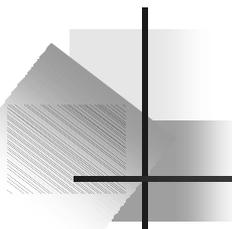


Privacy Considerations



Privacy Requirements

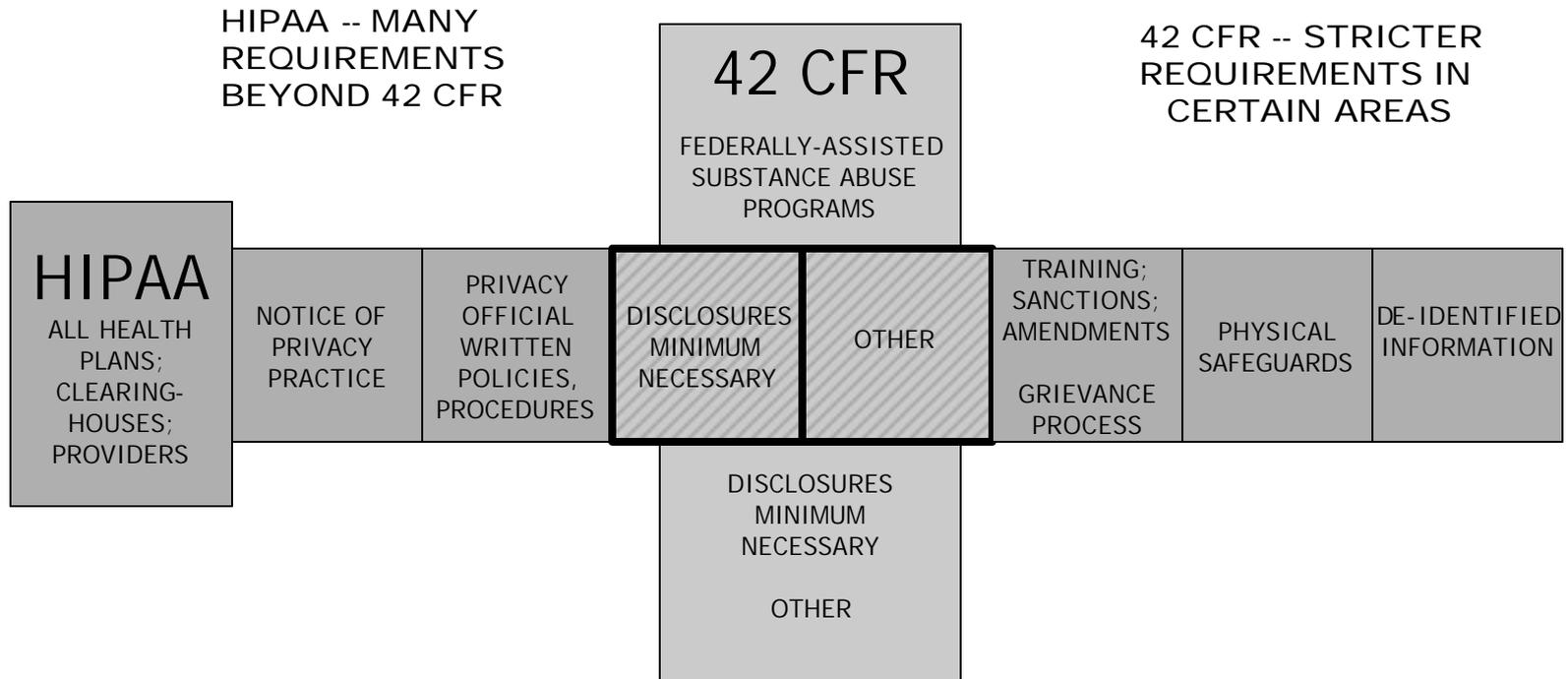
- 42 CFR contains general privacy protections for substance abuse patient records
- Most provisions are consistent with or more restrictive than HIPAA
- Many provisions are silent regarding administrative procedures and safeguards
- No significant conflicts exist

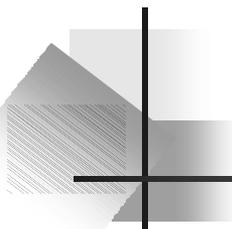


HIPAA Privacy and 42 CFR pt.2

- Entities subject to both will probably need additional administrative, technical, or policy safeguards, but will still follow the 42 CFR rules for when disclosure is allowable
- 42 CFR allows certain disclosures without patient consent including disclosures for medical emergencies, research, program audit or evaluation, and central registries
- HIPAA contains additional personnel designation and training requirements and would require similar safeguards for all types (written, electronic, or oral) of records

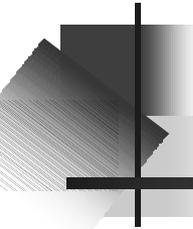
HIPAA and 42 CFR Overlap



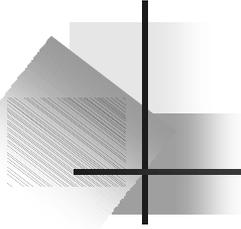


Privacy Considerations

- 42 CFR contains general privacy protections for substance abuse patient records
- Privacy screens

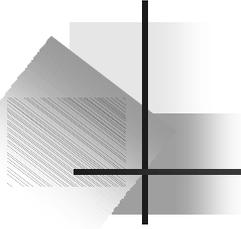


Security Technology-related Considerations



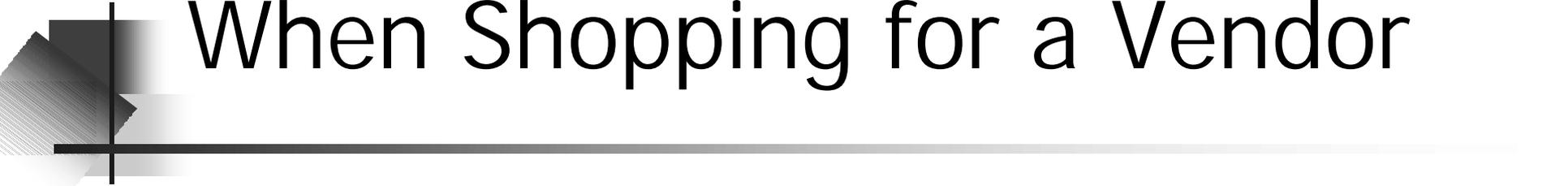
Security Requirements

- Ensure the confidentiality, integrity, and availability of all EPHI created, received, maintained, or transmitted
- Protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA
- Ensure compliance by its workforce

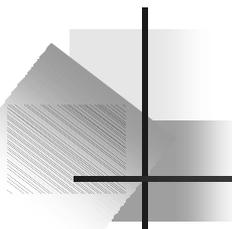


Security Considerations

- The costs of system security measures
- Compatibility with existing systems
- Ease of use of security features
- The availability of audit trails
- IT staffing, knowledge, and infrastructure

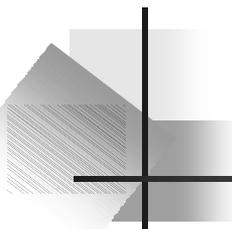


When Shopping for a Vendor



When Shopping for Technology...

- The technical capabilities of available software and systems
- Audit Controls (record and examine activity in information systems that contain or use EPHI at the data element level)
- Intrusion Detection Systems to identify possible network based intrusions, security breaches, and unauthorized access attempts
- Encryption (Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner)
- A central access control directory or mechanism (such as LDAP, etc.) that manages access to EPHI
- HL7 (for claims attachments)

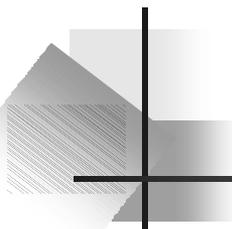


Discuss with the Vendor...

- Will your vendor be HIPAA compliant by the mandated deadlines?
- Will the software be compliant with the Transactions Addenda?
- If not, can a clearinghouse/translator solve your Transaction/Code Set issues?
- Do you have a crosswalk from standard code sets to ones used by your internal systems?
- Do you plan on internalizing standard code sets?

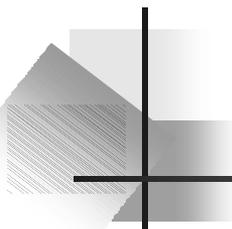
Top Questions to Ask Your Software Vendor

1. What software updates are needed for HIPAA compliance?
2. What release (version, patch) of your product supports the HIPAA claim (837) and remittance (835) transactions?
3. Does my practice / facility have to be at a particular release level to implement the HIPAA release or is this a complete upgrade from our current version?
4. What are your service level agreements for continued support?
 - New versions of transactions
 - Newly mandated transactions
5. Does the software support strip and store requirements?



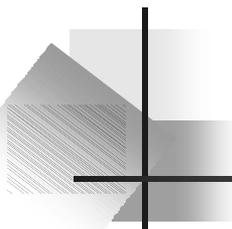
Top Questions to Ask Your Software Vendor

6. How does your product support collecting the required and situational claim data: via the screens used by our staff as they interact with patients or is this done on-line at a later time?
7. Will you support the required code sets?
8. Will the software let the practice exchange these transactions directly with payers, or do they have to go through a specific clearinghouse?
9. How much will this upgrade or new version cost our practice based upon the answers to the above questions?
10. When will the software updates be available?
11. How much lead time is required to install and test the software?
12. What is the minimum hardware requirement for servers and workstations to run the HIPAA compliant version?



Top Questions to Ask Your Software Vendor

13. What training, support and services are available to help my office?
14. Are there training and or consulting services available to help me test the HIPAA release?
15. What are your contingency plans if you cannot be ready on time?
16. Who specifically can I contact for HIPAA transactions questions?
17. Do you have crosswalks for my payers or your affiliated clearinghouses?
18. Can we choose a clearinghouse with the new version?
19. Do you have the companion guides for my payers with whom I file directly?

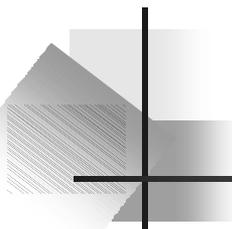


Top Questions to Ask Your Software Vendor

20. Do you have a list of the HIPAA data elements supported by the product?
 - a) Is this list transaction specific?
 - b) Does this list map to the current 1500 or UB92/1450 so we can see what new data we must develop?
21. Will your product or clearinghouse support HIPAA specific business edits?
22. How is the production of the 837 supported by your product?
23. Can I upgrade to the various standards incrementally?

Top Questions to Ask Your Software Vendor

24. Does the product support automatic posting using the 835-remittance transaction?
25. Do you belong to any of the HIPAA-related workgroups? How do you remain current on the latest HIPAA developments?
26. Has your testing process included all of the seven types recommended by WEDI SNIP?
27. Has the software received third-party certification that it can generate HIPAA compliant transactions?
28. Will you send me a testing schedule that includes:
 - Internal testing
 - Testing with Medicare
 - Testing with commercial payers
 - Testing with a clearinghouse (if applicable)

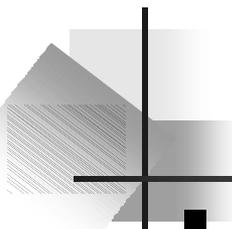


Check List - Billing/Practice Management Vendors

- Which transactions can the software/system send and/or receive?
- Which of your trading partners has tested the transactions for the software/system?
- What types of tests has the software/system been through?
- Does the software/system support the collection of all new required and situational elements?

Check List - Billing/Practice Management Vendors

- Does the software/system have controls to prevent the entry of non-compliant values?
- Does the software/system have look-up fields for codes and other values that are regularly updated to current HIPAA required code standards?
- What is the maintenance and update schedule for all codes sets in the software/system?
- Does the software/system have adequate security for sending/receiving transactions?



Check List - Billing/Practice Management Vendors

- Has the software/system been certified?
- Can you find out the experience of others who have used the system?
- How many testing partners and tests have been performed? What were the results?
- Have tests been performed on both inbound and outbound transactions?
- What system support is available? Is it documented in the agreement?