ctg

HealthCare Solutions

Session 4.01:

Contingency Planning for HIPAA Transactions and Code Sets

Christine Stahlecker, Principal Consultant
Computer Task Group Healthcare Solutions
WEDI SNIP Co-Chair
HL7 A-SIG Co-Chair

Today's Agenda

Contingency Planning for HIPAA Transactions and Code Sets

ctg HealthCare Solutions

1. Quick mandate re-cap
2. What is the impact from the Guidelines?
3. Contingency Planning Definitions and Terms
4. Making a COOP
5. But, will it fly?

Mandate Recap

- Privacy compliance by April 14, 2003
- Testing the Transactions and Code Sets (TCS) by April 16, 2003
- Full TCS implementation by October 16, 2003
- Security by April 21, 2005 or 2006 for small payers
- Not yet specified:
    1. National Provider ID – Final Rule due 4Q 03
    2. Health Plan ID – Draft Rule due 2Q 04
    3. Claims Attachments – Sometime in 2004
    4. First Annual Update to all TCS; ongoing

What's the real status?

Transactions & Code Sets

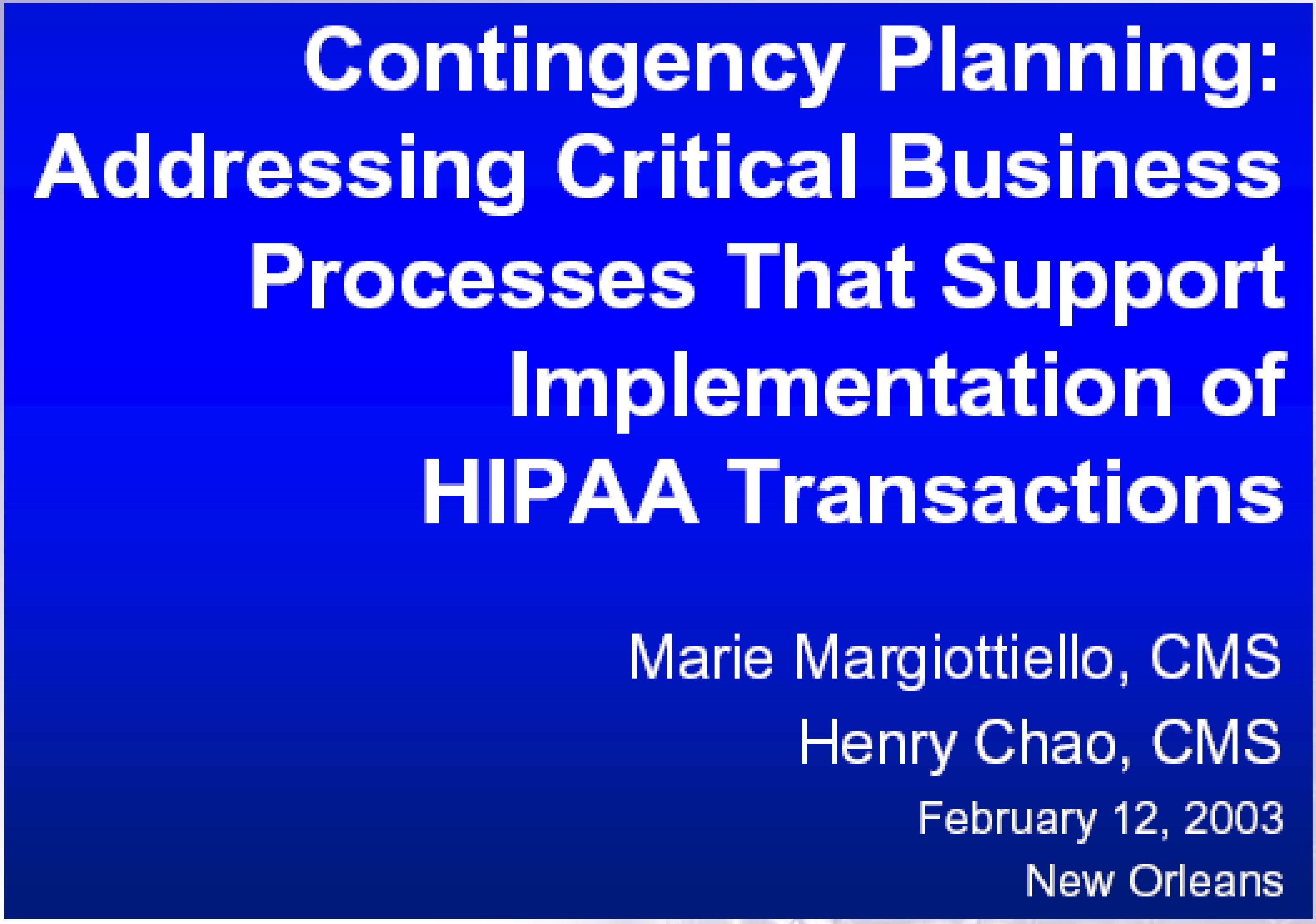
- The industry is <u>not ready</u> for a cut over
- Health Plans are testing the claim and remittance; many are still tweaking companion guide edits
- Vendors still tweaking software releases
- Clearinghouses working their way through <u>their</u> list of major payers
  - Each payer may have customized edit requirements = Companion Guides
  - Dispute whether Provider-Payer test needed and may not support it
- Providers need to test with payers but many do not have complete solutions in place or an electronic pathway to reach payers

Impact from the Guidelines

- Guidance given by CMS on July 24
- Guidance opened the door for payers to have a parallel path (old + new formats)
- Intent was 'support' but also created 'pain'
  - Payers now have another option: need to review capabilities, inform trading partners
  - Providers now need to find out what payers will do
  - *Outreach and Test; Outreach and Test; Outreach and Test*
  - Can the vendors and clearinghouses operate in dual path?
  - Will the 'as-is' path really be the same as today?

Impact from the Guidelines

- Guidance outlined how CMS would ‘enforce’
  - Enforcement is to be *complaint driven*
  - Investigate both trading partners
  - Look for what was done pre/post Oct 16 to get ready to comply
  - If providers’ vendors or clearinghouses are not ready, told to *vote with their feet*
    - Provider and Payer hold the responsibility
    - Impractical to switch delivery chain now
    - Need to document good faith efforts to comply
    - Need to prepare contingencies, rationale and contingency deployment criteria documented



Contingency Planning: Addressing Critical Business Processes That Support Implementation of HIPAA Transactions

Marie Margiottiello, CMS

Henry Chao, CMS

February 12, 2003

New Orleans

Definitions (see the Reference slides)

- Disaster Recovery Plan
- Disaster Recovery Planning
- Contingency Plan
- Contingency Planning
- Continuity Of Operations Plan (COOP)

Risk Analysis

- How likely is it for this situation to occur?

And

- What impact would it have?

Risk Analysis

ctg HealthCare Solutions

- **Based on specific probability and criticality factors**
  - **Product of: (probability) x (criticality)**
  - **Probability: chance that the future event will occur (if happening now, it's a problem, not a risk)**
  - **Criticality: the impact of a future event**

    (no impact = no risk)

Risk Analysis

- Identify the degree of probability:
  - High – nearly certain (80 – 99%)
  - Mid – probable, possible (20 – 80%)
  - Low – improbable (< 20%)

Risk Analysis

- Identify the degree of criticality
  - High – total failure or serious degrading of business function
  - Moderate – impaired performance
  - Low – little impact, but more than none

Risk Analysis

- Analyze and assess the relative risk
- Identify the critical business processes
- For each, identify potential points of failure
- Identify impact to users, business units and extended work flows

Business Impact Analysis

- Identify business processes affected if failure occurred
- Determine failure-tolerance level for each function (e.g. degradation, disruption, completely unavailable)
- What-if; how bad would it be?
- Determine risk-avoidance activities to be taken on varying levels of tolerance

Business Impact Analysis

- Document risk analysis (description and rationale)
- Prioritize the listing of critical business processes
  - Business processes should be identified, evaluated, and then ranked in order of importance

Business Impact Analysis

Business Process: Provider Claim Submission

Dependency	Probability	Duration	Criticality Factor	Total Risk Score
Clearinghouse not ready				
Payer X requires standard so HIS must ‘go live’				
Medicaid not ready so we must continue legacy format				
Scope creep: HIS Medicaid output needs to be converted back to UB92				

Business Impact Analysis

Business Process	Number of Patients Scheduled, Registered	Number of Patients Seen	Number of Claims Submitted (by Payer)	Total of Submitted Charges (by Payer)	Error Claims Returned (by Error, Payer)	Days to Correct and Resubmit	Total Score
BP #1							
BP #2							
BP #3							
and so on…							

Identification of Alternatives

- **For each critical business process, identify possible alternative workflows**
- **Select the best-fit alternative for each mission critical business process or scenario**

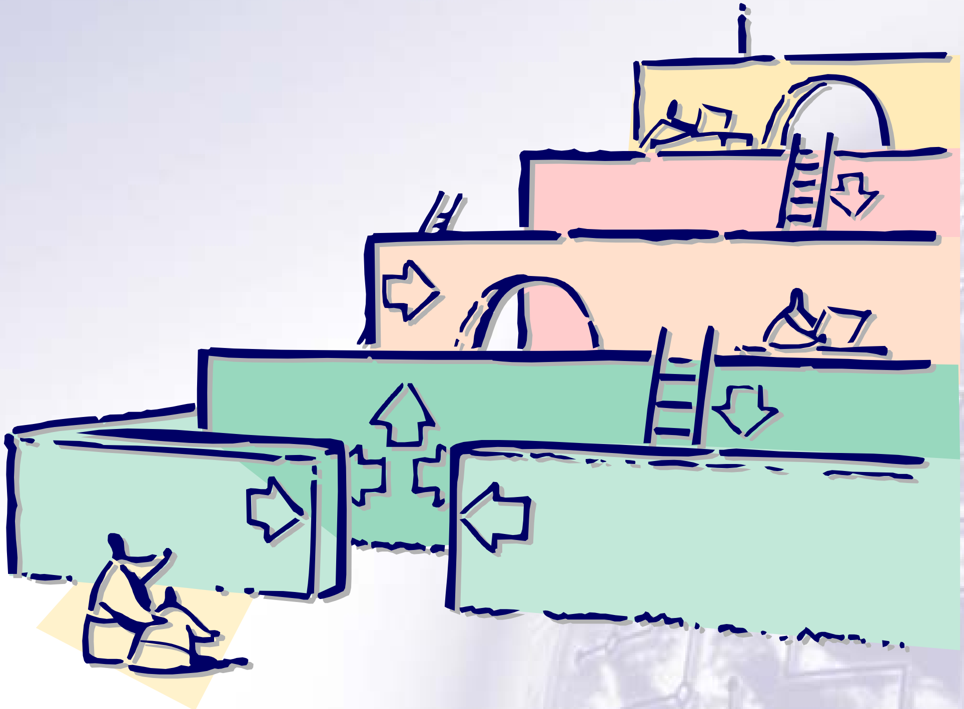
Develop the COOP

Continuity of Operations Plan

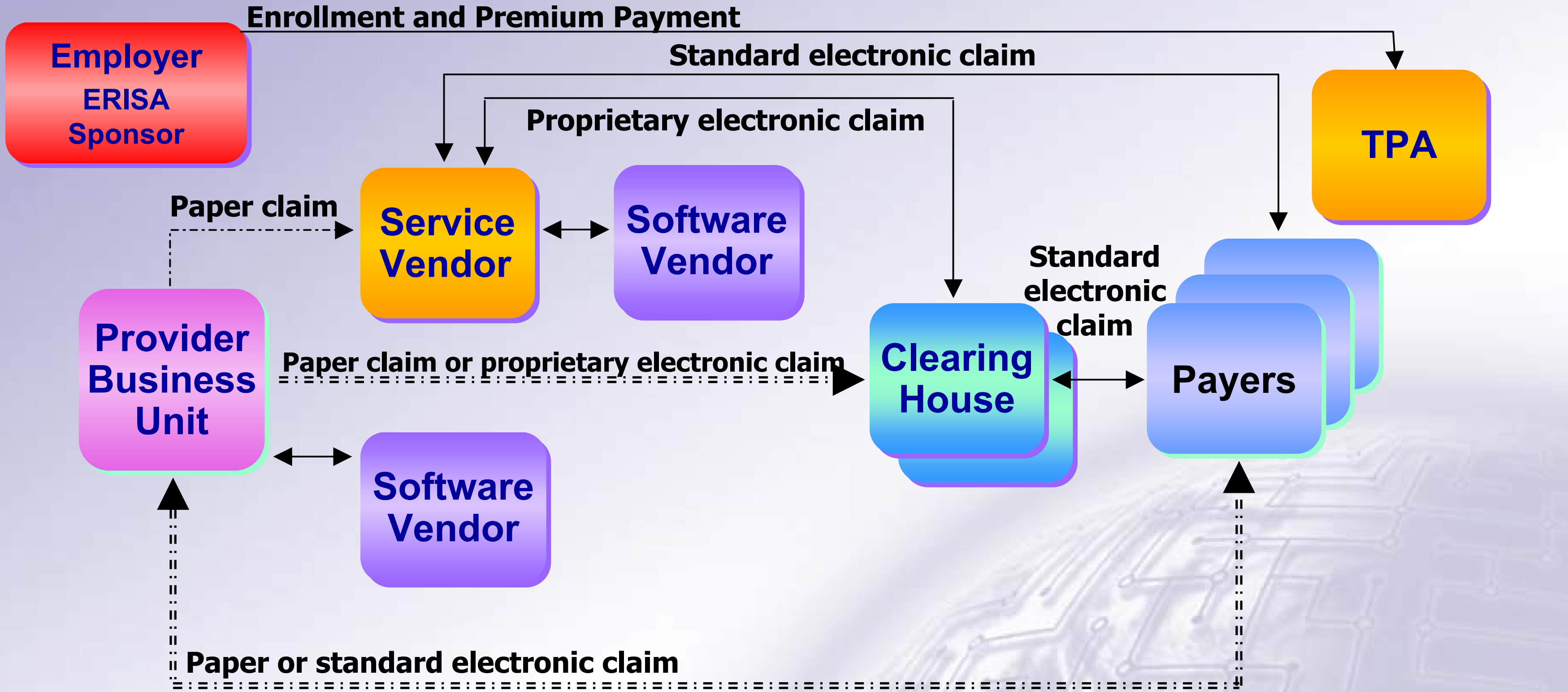
- Each contingency needs to specify:
  - Assumptions (baseline parameters for planning)
  - Triggers (indication of failure, rationale to activate the alternative process)
  - Notification (who to tell)
  - Resource Assignments (who does what)
  - Procedures (the work-around)
  - Duration (for how long)
  - Monitoring (see how it goes)

But will it fly?

- Contingency planning is based on *what-if* thinking
- You need a wide range of subject matter expertise on current processes, scope



Claim Transaction Model


Enrollment and Premium Payment
Employer
ERISA
Sponsor
TPA
Standard electronic claim
Proprietary electronic claim
Paper claim
Service Vendor
Software Vendor
Standard electronic claim
Provider Business Unit
Paper claim or proprietary electronic claim
Clearing House
Payers
Software Vendor
Paper or standard electronic claim

Electronic ⟷

Paper ⟷

Manual, Paper & Electronic ⟷

Legend

🟧 Business Associate

🟪 Provider Covered Entity

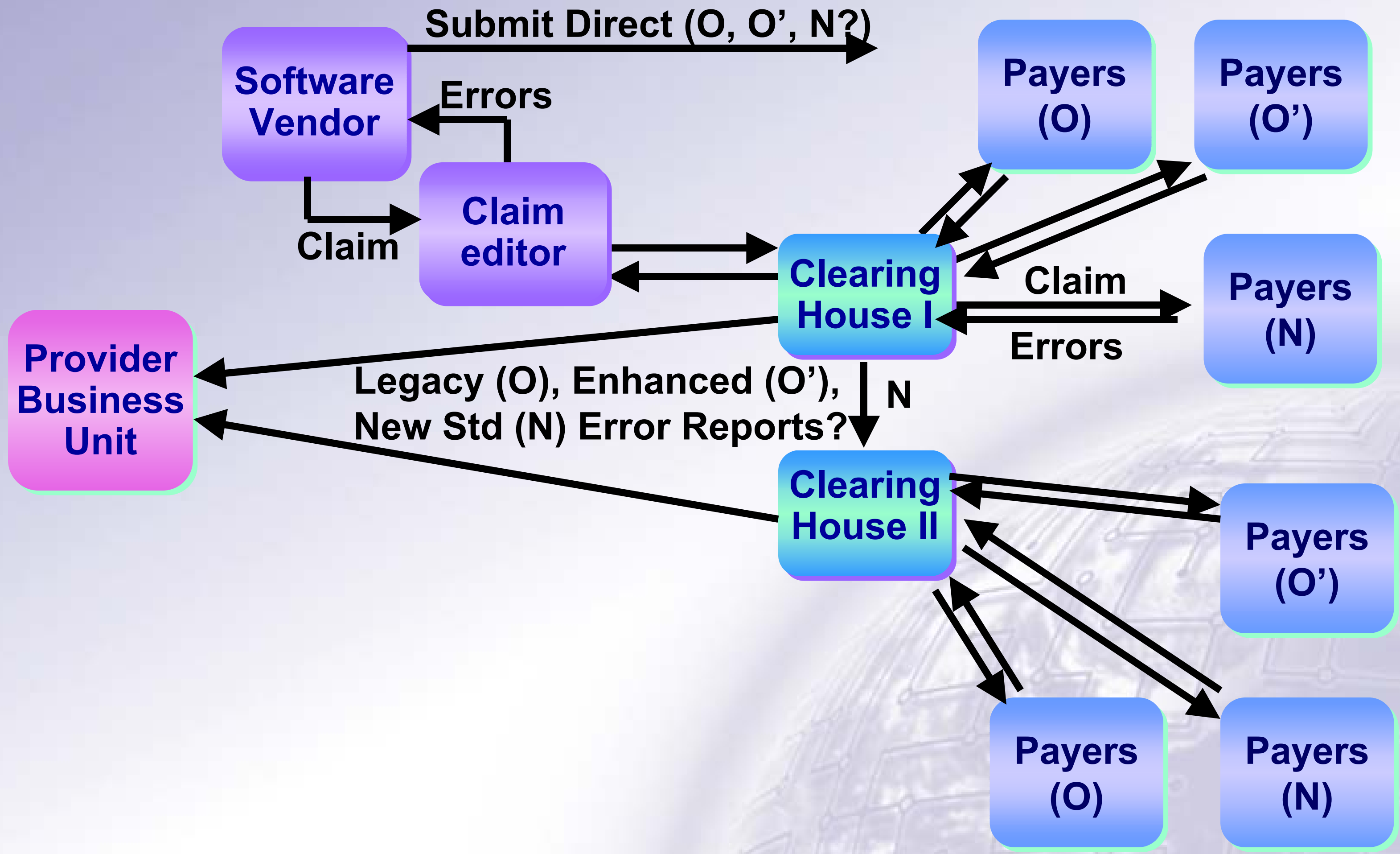
🟪 Software Vendors

🟦 Clearinghouse Covered Entity

🟦 Health Plan Covered Entity

🟥 Employer as Health Plan Covered Entity

Claim Submission and Error Return Formats?



Stakeholder Checklist

Will it Fly?

Checklist Questions - Payer

- ✓Will multiple formats be allowed from a trading partner during the transition?
- ✓How long will this dual-path capability be available on a ‘need to use’ basis?
- ✓Can a provider revert prior to October 16, 2003? after October 16, 2003?
- ✓What are your specific LOB requirements? Are there separate Companion Guides? Are there separate decisions regarding dual-path?

Will it Fly?

Checklist Questions - Payer

- ✓ Is the legacy option really going to be exactly the same as today’s processing?
- ✓ Are there recommended ‘phase in’ strategies?
- ✓ Do you offer test support (e.g. Help Desk)? How long should I wait for a reply before I follow up with your Help Desk on an issue?
- ✓ If my clearinghouse ‘goes live’ with you, do I control whether legacy or new standard format is used for my claims? Is my authorization required?

Will it Fly?

Checklist Questions - Provider

- ✓ Do you know how all of your claims are delivered to payers? (e.g. e-pathways by payer)
- ✓ Have you reviewed payers' front end reports to know whether your staff needs training to be able to correct and resubmit claims?
- ✓ Have all of the data capture points been updated for the new required data elements (e.g. screens, interview questions, keying habits)?

Will it Fly?

Checklist Questions - Provider

- ✓ If you use a clearinghouse, do you control whether the legacy pathway or new standard is used to reach individual payers?

  Heads up: some providers are experiencing unexpected claim returns ***right now*** due to clearinghouse-payer upgrades.

- ✓ Are the payers that your vendor/clearinghouse tested with, the same payers that are important to you? Consider the various Lines Of Business.

Will it Fly?

Checklist Questions - Provider

- ✓ Will your vendor, clearinghouse, BA enable/support your testing with payers? If not, are they guaranteeing reimbursement?
- ✓ Are you interested in a direct connection?
- ✓ Exactly what does the HIPAA compliant version NOT include? What are your options to implement these other transactions?
- ✓ Are there more releases or versions required from your vendor to supply all of the capabilities of the standard transactions (e.g. is MSP/COB included now or another release – may need to reserve budget now)?
- ✓ Have you established a HIPAA test environment, team, coordinator, plan?

Will it Fly?

Checklist Questions - Vendor

- ✓What version is your customer *really* using? Are any backlogged updates required?
- ✓Have you certified your products? In an on-going basis?
- ✓Are you recommending that your customers certify?
- ✓Can others help with your customization, deployment, testing?

Will it Fly?

Checklist Questions - Clearinghouse

- ✓ When will you test with my Payers?
- ✓ Can I control when my claims are delivered to individual payers in the new standard (e.g. default to legacy until I say ok for my claims)?
- ✓ Are you testing with other Clearinghouses? If my claims follow that e-pathway, will you report status to me?
- ✓ How many must be tested before you get to my key payers – what is the schedule?
- ✓ What will the claims error notification look like? Will you conform all payers' error reports for consistency or will I need to work with multiple formats and interpretations?

Best Practices - TCS

- Certify. Test with one of the certification services. This may be proof that you can create compliant transactions.
- Complete internal testing and certification before testing with your trading partners.
- Plan to test; prepare to test; follow your plan.
  - Using current production data is not sufficient.
  - Use selective, specific Test cases
  - Consider a production parallel (if supported by your payers) to really be able to compare future adjudication results

Best Practices - TCS

- Certification is very useful and demonstrates ‘good faith effort’ to comply:
  - Certification facilitates Unit Testing of key Inputs and Outputs
  - Unit Testing should focus on controlled test cases, scenarios and predicted results
  - Unit Test is limited in the volume of transactions
  - Certification Facilitates System Testing
  - May be used to ‘stress test’ with large volumes of transactions
  - Certification Facilitates User Acceptance Testing
  - Cases address Companion Guide edit criteria
- Certification Does Not Replace Provider-Payer testing

Best Practices - TCS

- ‘Hands off’ testing made available between CEs
- Use of production programs in test cycles for actual results
- ‘Migrate’ the workload to new TCS rather than cut-over
- Business processes need to be addressed, it is not just the computer
- Streamlined error correction, not just the original submission
- Build test systems to last (internal thru external) – we will need them annually
    - Provider Identifier is expected next

Avoid Cash Flow *Brown-Out*

- ***Even if you're on the right track, you'll get run over if you just sit there.***

  Will Rogers, Humorist

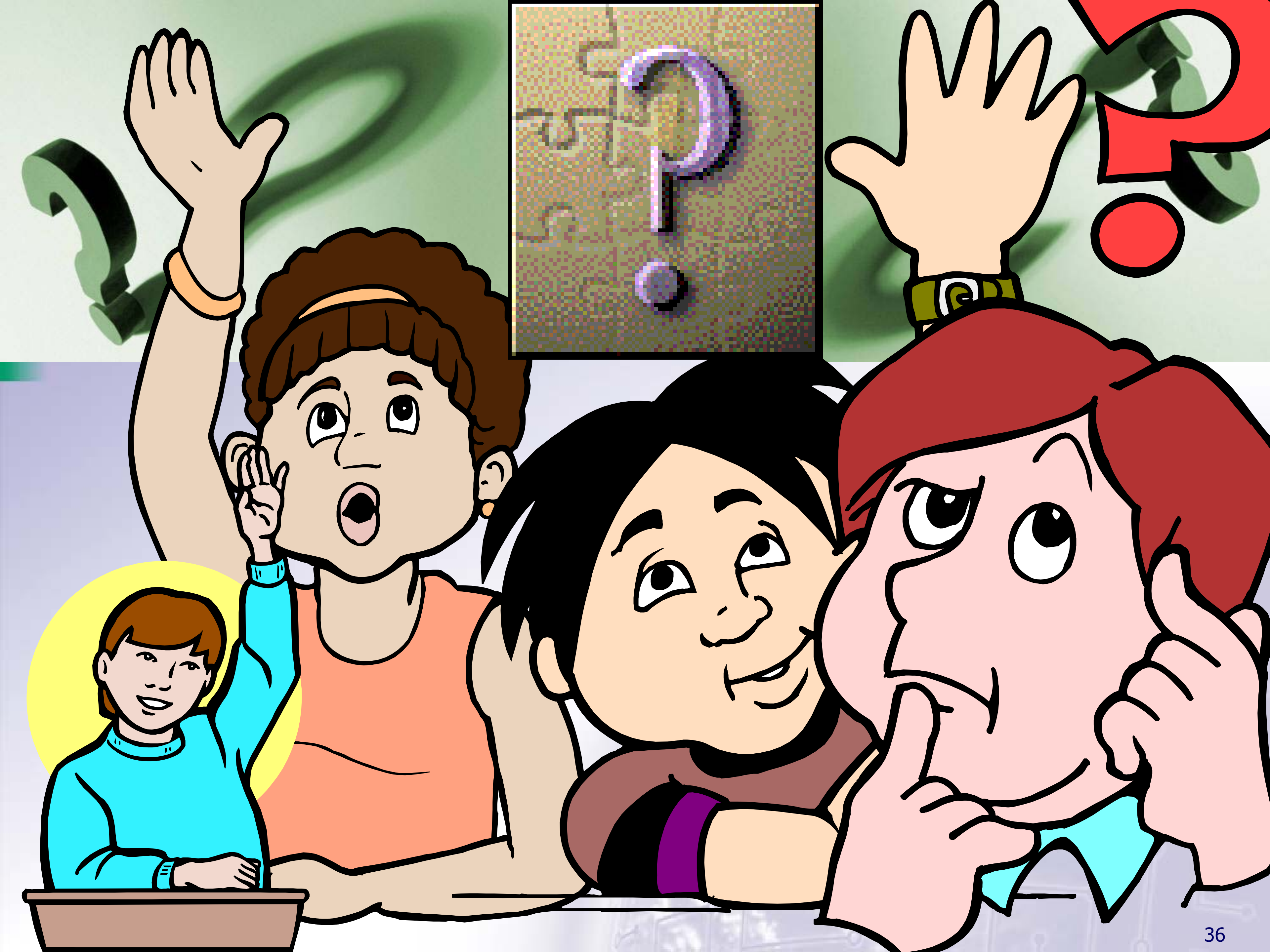
- ***Bad news early is good news. [On early problem detection].***

  Shamelessly stolen from Empire BCBS

- **Assure yourselves – know your performance baseline; anticipate changes; monitor closely**

Dependencies

- Do not be the *weakest link*
- Failure will not be a singular event.
- We are in this together.



ctg
HealthCare Solutions

Session 4.01:

Contingency Planning for HIPAA Transactions and Code Sets

Christine Stahlecker, Principal Consultant

Computer Task Group Healthcare Solutions

WEDI SNIP Co-Chair

HL7 A-SIG Co-Chair

Additional Points of Interest and Reference

CMS FAQs Recently Posted

- How will Medicare decide whether to implement its contingency plan?
- Who will determine whether I made a good faith effort?
- What kind of activities is Medicare doing to demonstrate good faith efforts?
- Is it acceptable for a health plan to announce its contingency now?
- What will Medicare's contingency plan be?

What is an acceptable contingency plan?

- An acceptable contingency plan is whatever is appropriate for the individual plan's situation in order to ensure the smooth flow of payments. Health plans will need to make their own determinations regarding contingency plans based on their unique business environments. A contingency plan could include, for example, maintaining legacy systems, flexibility on data content or interim payments. Other more specific contingency plans may also be appropriate. For example, a plan may decide to continue to receive and process claims for supplies related to drugs using the NCPDP format rather than the 837 format currently specified in the regulations. The appropriateness of a particular contingency or the basis for deploying the contingency will not be subject to review.

What will Medicare’s contingency plan be?

- Medicare’s contingency would be to continue to accept and send transactions in legacy formats – in addition to HIPAA compliant transactions - while trading partners work through issues related to implementing the HIPAA standards. The contingency plan will be the same for all Medicare’s fee-for-service contractors. A decision on whether to deploy a contingency will be made by September 25, 2003. Medicare will continue its active outreach and testing efforts to bring its trading partner community into compliance with the HIPAA standards.

How does a covered entity demonstrate good faith?

- Covered entities should keep track of the efforts they have made – both before and after the October 16 compliance date – to become compliant. For a provider, that could include your efforts to work with vendors, clearinghouses and submitters to schedule testing with plans, and the results of those tests. For a plan, it could include keeping track of outreach activities (letters, conferences, phone calls, etc.) encouraging providers/submitters to schedule testing, testing schedules, and statistics showing increased testing results.

Will Medicare be ready on October 16, 2003?

- Yes. Medicare already accepts HIPAA-compliant transactions.

How will Medicare decide whether to implement its contingency plan?

- CMS is currently assessing the readiness of our trading partner community including the number of Medicare submitters who are testing and in production with our contractors. The results of these indicators will determine whether CMS will deploy its contingency.

Is it acceptable for a health plan to announce its contingency now?

ctg HealthCare Solutions

- Yes. Health plans should announce their contingency plans as soon as possible to allow their trading partners enough time to make any needed adaptations to their business operations to ensure minimal disruptions. In deciding whether to deploy a contingency plan, organizations would have to make an assessment of their outreach and testing efforts to assure they made a “good faith” effort.

Who will determine whether I made a good faith effort?

- The Office of HIPAA Standards within the Centers for Medicare & Medicaid Services (CMS) is responsible for enforcing the electronic transactions and code sets provisions of the law. When OHS receives a complaint about a covered entity, it would ask the entity to demonstrate their reasonable and diligent efforts to become compliant and, in the case of health plans, to facilitate the compliance of their trading partners. Strong emphasis will be placed on sustained actions and demonstrable progress in determining a covered entity’s good faith effort.

What kind of activities is Medicare doing to demonstrate good faith efforts?

- CMS has directed the Medicare contractors to intensify all HIPAA outreach and testing efforts with their respective provider and submitter communities and trading partners. Contractors are communicating HIPAA information via individual provider contacts, published provider bulletins, websites, and many other mechanisms. CMS also provides HIPAA information via webcasts, videos, advertising in industry publications, and audio conferences.

Does the law require Medicare claims to be submitted electronically after Oct. 2003?

ctg HealthCare Solutions

- ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003.
- The Secretary may grant a waiver from this requirement.
- The Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies.
- Beneficiaries will also be able to continue to file paper claims if they need to file a claim on their own behalf.
- Medicare published an interim Final Rule on August 15. The open comment period closes October 14, 2003 5PM. The effective date is October 16, 2003.
- Reasons paper may continue include: roster billing, Medicare demonstration projects, multiple payers preceding Medicare.

Are small providers exempt from HIPAA?

- No. If a provider transmits any of the designated transactions electronically, it is subject to the HIPAA Administrative Simplification requirements regardless of size. Small providers are exempt from the ASCA provision that excludes paper claims from Medicare coverage effective October 16, 2003. Small providers will be able to continue to submit paper claims. ASCA defines a small provider or supplier as:
  - a provider of services with fewer than 25 full-time equivalent employees or
  - a physician, practitioner, facility or supplier (other than provider of services) with fewer than 10 full-time equivalent employees.

Note: **this provision does not preclude providers from submitting paper claims to other health plans.**

What will the enforcement process look like?

- The enforcement process for HIPAA transactions and code sets (and for security and standard identifiers when those are adopted) will be primarily complaint-driven. Upon receipt of a complaint, CMS would notify the provider of the complaint, and the provider would have the opportunity to demonstrate compliance, or to submit a corrective action plan. If the provider does neither, CMS will have the discretion to impose penalties.

- Our enforcement strategy will concentrate on achieving voluntary compliance through technical assistance. Penalties would be imposed as a last resort.

Definitions

- **Disaster Recovery Plan:** The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

Source: Disaster Recovery Journal

Definitions

- **Contingency Plan:** A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement, or replacement resources.

Source: Disaster Recovery Journal

Definitions

- **DISASTER RECOVERY PLANNING:** The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster.

  SIMILAR TERMS: Contingency Planning; Business Resumption Planning; Corporate Contingency Planning; Business Interruption Planning; Disaster Preparedness.

Source: Disaster Recovery Journal

Definitions

ctg HealthCare Solutions

- **CONTINGENCY PLANNING:** Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.

Source: Disaster Recovery Journal

Definitions

A **Continuity Of Operations Plan** provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. This term traditionally is used by the Federal Government and its supporting agencies to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.

Source: Disaster Recovery Journal

HIPAA Roundtable & Audio Conferences

- **The Thirteenth National HIPAA Implementation Roundtable is scheduled for Thursday September 25, 2003 from 2:00 – 3:30 PM ET.**
- **The call in number is 1-877-381-6315. The conference identification number is 1596442. NO registration required.**