A Systematic Method for Acquiring Regulatory Requirements: A Frame-based Approach

Travis D. Breaux and Annie I. Antón
North Carolina State University

RHAS-6, New Delhi, India, October 15th 2007

Presentation Outline

- High Assurance and Due Diligence
- U.S. Federal Regulatory Processes
- Challenges to Compliance
  - Acquiring Regulatory Requirements
    - Ambiguity
    - Traceability
- The Frame-Based Req'ts Analysis Method (FBRAM)
  - Upper Ontology
  - Context-free Markup
  - Document Model
  - Requirements

High Assurance and Due Diligence

In requirements engineering, *high assurance* is…

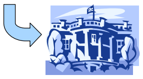
- The need for compelling evidence to demonstrate that systems satisfy critical properties such as accessibility, availability, security, etc.

In U.S. law, *due diligence* means…

- Reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations, *Black's Law Dictionary, 8th Edition*

U.S. Federal Regulatory Processes

U.S. Congress ratifies statutes



Executive branch agencies
(FAA, FCC, FDA, HHS, etc.)
develop regulations

Industry creates standards that support regulations
Industry and government perform regulatory audits

U.S. Federal courts decide:
(1) industry compliance with regulations
(2) regulatory compliance with statutes
(3) statutory compliance with the Constitution

Challenges to Compliance

Industry, auditors and regulators need methods to:

- Acquire an industry-wide, standard set of requirements from statutory goals, regulations and case law
- Coordinate changes to these requirements
- Select which requirements are relevant to their practices
- Develop measurable evidence of implementations

The evidence (including process and software artifacts) must:

- Demonstrate due diligence
- Provide a defensible position in a U.S. court of law

Acquiring Regulatory Requirements

Challenges to acquisition include…

- Intended Ambiguity

  From HIPAA §164.304: A *workstation* means "a laptop or desktop computer, or any other device that performs similar functions"
- Unintended ambiguity
  - Logical
  - Attributive
  - Referential
- Traceability and interpretations

Logical Ambiguity

- *Logical ambiguity* includes how English conjunctions "and" and "or" are assigned to logical connectives

  From HIPAA §164.524(a)(1): an individual has "a right of access to inspect and obtain" a copy of their protected health information

Attributive Ambiguity

- *Attributive ambiguity* refers to phrases that may be reasonably ascribed to more than one other phrase within a sentence

  From HIPAA §164.520(b)(1)(vii), "The [privacy] notice must contain the name or title and telephone number of a person or office"

  Could be construed to mean either…

  1. The name of a person or office
  2. The name and telephone number of a person or office
  3. The title and telephone number of a person or office

Referential Ambiguity

- *Referential ambiguity* occurs when a word refers to two or more:
  - Concepts, called intensional polysemy
  - Individuals or instances, called extensional polysemy
- Anaphoria and cataphoria are cases of extensional polysemy.
  - These include pronouns (it, they, such, etc.) that refer to individuals described earlier or later in a sentence or paragraph

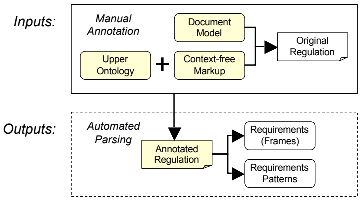
Traceability

- *Traceability* means the maintenance of forward and backward links between software artifacts.
- Regulatory requirements, at minimum, require traceability to originating paragraphs in regulations.

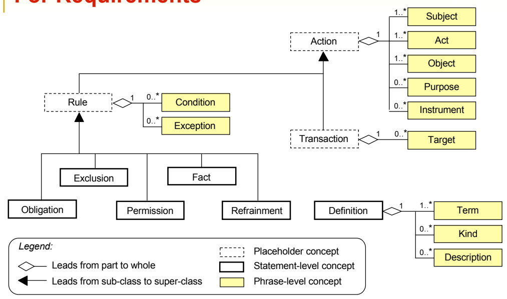
  Because ambiguities cannot be removed from regulations (only interpreted), traceability includes documenting these interpretations!

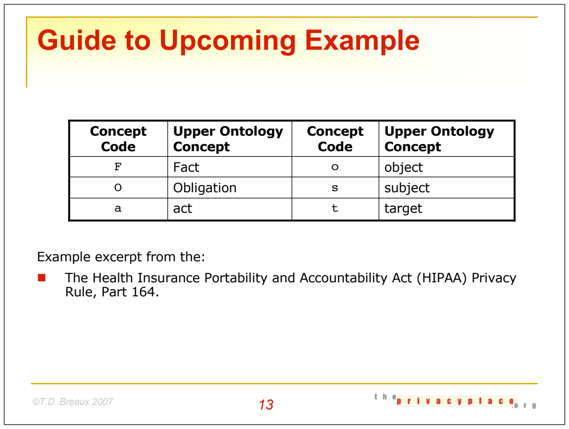
A Frame-based Approach

The Frame-Based Requirements Analysis Method (FBRAM)



Standard Upper Ontology
For Requirements



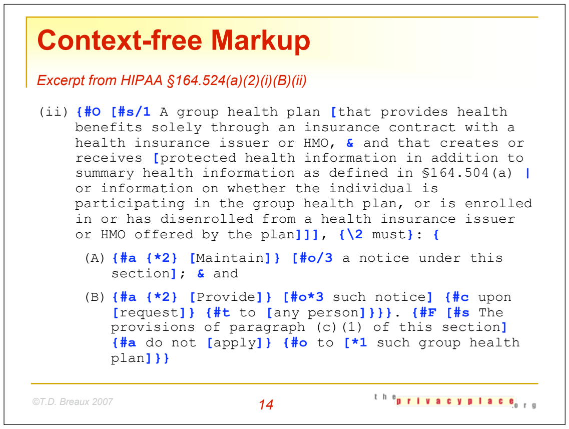


Guide to Upcoming Example

Concept Code	Upper Ontology Concept	Concept Code	Upper Ontology Concept
F	Fact	o	object
O	Obligation	s	subject
a	act	t	target

Example excerpt from the:

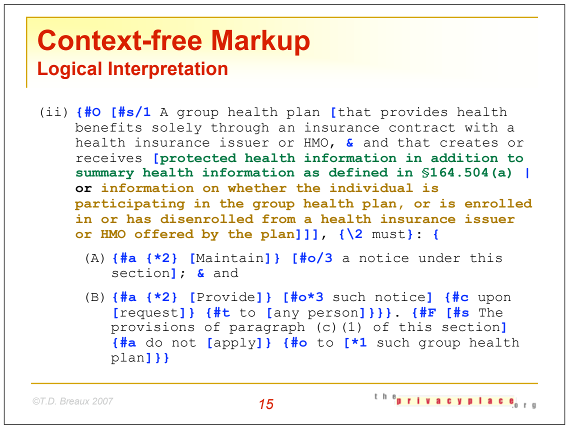
- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, Part 164.



Context-free Markup

Excerpt from HIPAA §164.524(a)(2)(i)(B)(ii)

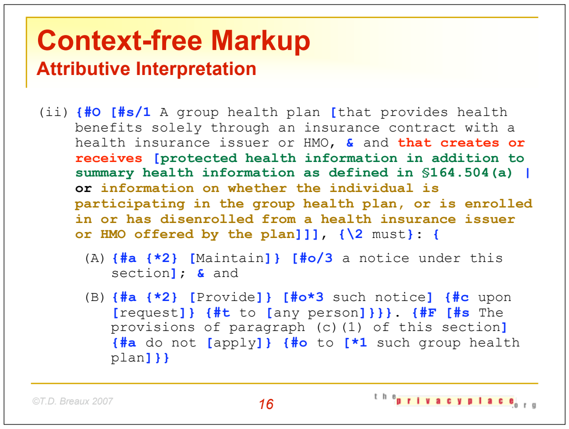
```
(ii) {#O [#s/1 A group health plan [that provides health
     benefits solely through an insurance contract with a
     health insurance issuer or HMO, & and that creates or
     receives [protected health information in addition to
     summary health information as defined in §164.504(a) |
     or information on whether the individual is
     participating in the group health plan, or is enrolled
     in or has disenrolled from a health insurance issuer
     or HMO offered by the plan]]], {\2 must}: {
   (A) {#a {*2} [Maintain]} [#o/3 a notice under this
       section]; & and
   (B) {#a {*2} [Provide]} [#o*3 such notice] {#c upon
       [request]} {#t to [any person]}}}. {#F [#s The
       provisions of paragraph (c)(1) of this section]
       {#a do not [apply]} {#o to [*1 such group health
       plan]}}
```



Context-free Markup

Logical Interpretation

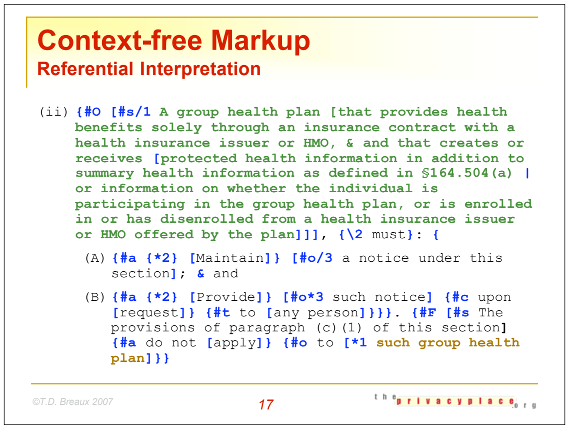
```
(ii) {#O [#s/1 A group health plan [that provides health
     benefits solely through an insurance contract with a
     health insurance issuer or HMO, & and that creates or
     receives [protected health information in addition to
     summary health information as defined in §164.504(a) |
     or information on whether the individual is
     participating in the group health plan, or is enrolled
     in or has disenrolled from a health insurance issuer
     or HMO offered by the plan]]], {\2 must}: {
   (A) {#a {*2} [Maintain]} [#o/3 a notice under this
       section]; & and
   (B) {#a {*2} [Provide]} [#o*3 such notice] {#c upon
       [request]} {#t to [any person]}}}. {#F [#s The
       provisions of paragraph (c)(1) of this section]
       {#a do not [apply]} {#o to [*1 such group health
       plan]}}
```



Context-free Markup

Attributive Interpretation

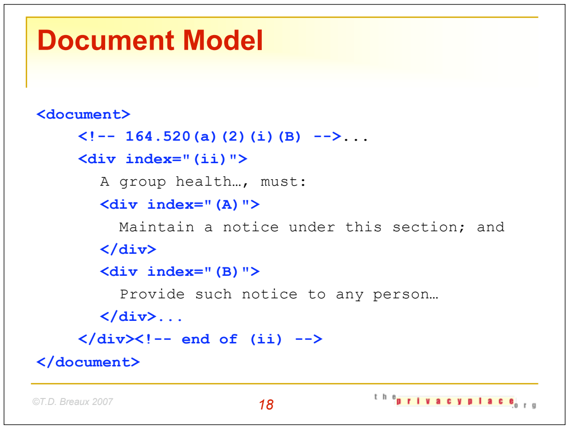
```
(ii) {#O [#s/1 A group health plan [that provides health
     benefits solely through an insurance contract with a
     health insurance issuer or HMO, & and that creates or
     receives [protected health information in addition to
     summary health information as defined in §164.504(a) |
     or information on whether the individual is
     participating in the group health plan, or is enrolled
     in or has disenrolled from a health insurance issuer
     or HMO offered by the plan]]], {\2 must}: {
   (A) {#a {*2} [Maintain]} [#o/3 a notice under this
       section]; & and
   (B) {#a {*2} [Provide]} [#o*3 such notice] {#c upon
       [request]} {#t to [any person]}}}. {#F [#s The
       provisions of paragraph (c)(1) of this section]
       {#a do not [apply]} {#o to [*1 such group health
       plan]}}
```



Context-free Markup

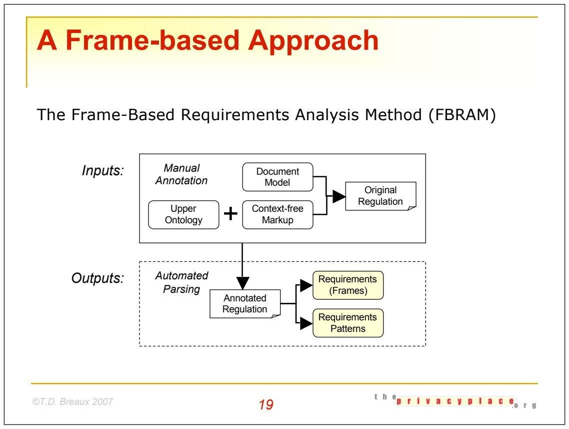
Referential Interpretation

```
(ii) {#O [#s/1 A group health plan [that provides health
     benefits solely through an insurance contract with a
     health insurance issuer or HMO, & and that creates or
     receives [protected health information in addition to
     summary health information as defined in §164.504(a) |
     or information on whether the individual is
     participating in the group health plan, or is enrolled
     in or has disenrolled from a health insurance issuer
     or HMO offered by the plan]]], {\2 must}: {
   (A) {#a {*2} [Maintain]} [#o/3 a notice under this
       section]; & and
   (B) {#a {*2} [Provide]} [#o*3 such notice] {#c upon
       [request]} {#t to [any person]}}}. {#F [#s The
       provisions of paragraph (c)(1) of this section]
       {#a do not [apply]} {#o to [*1 such group health
       plan]}}
```



Document Model

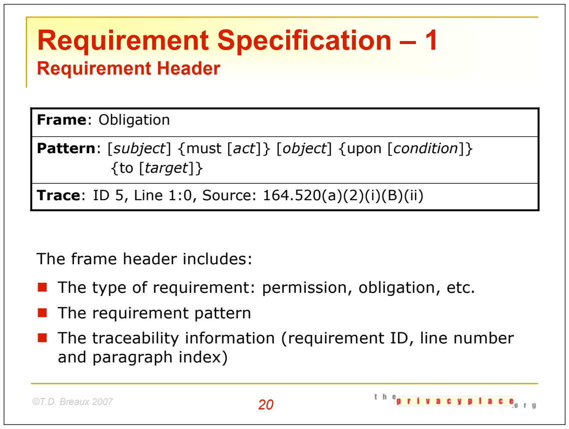
```
<document>
    <!-- 164.520(a)(2)(i)(B) -->...
    <div index="(ii)">
      A group health…, must:
      <div index="(A)">
        Maintain a notice under this section; and
      </div>
      <div index="(B)">
        Provide such notice to any person…
      </div>...
    </div><!-- end of (ii) -->
</document>
```



A Frame-based Approach

The Frame-Based Requirements Analysis Method (FBRAM)

Inputs:
Manual Annotation
Document Model
Original Regulation
Upper Ontology
+
Context-free Markup
Outputs:
Automated Parsing
Annotated Regulation
Requirements (Frames)
Requirements Patterns



Requirement Specification – 1

Requirement Header

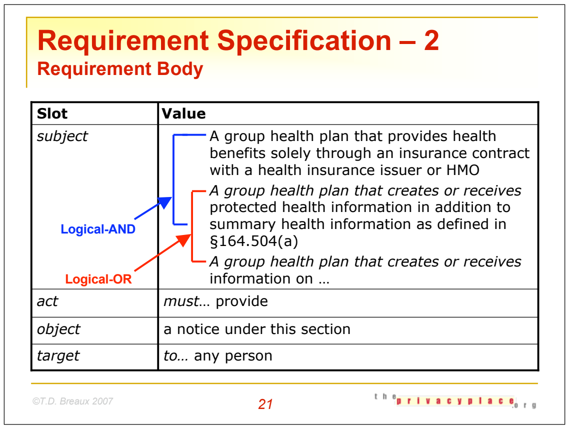
Frame: Obligation

Pattern: [*subject*] {must [*act*]} [*object*] {upon [*condition*]}
{to [*target*]}

Trace: ID 5, Line 1:0, Source: 164.520(a)(2)(i)(B)(ii)

The frame header includes:

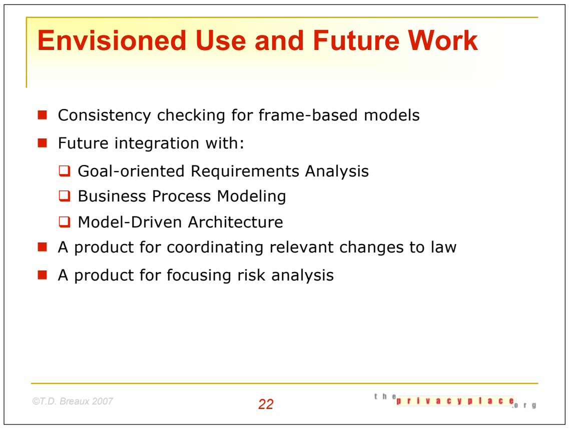
- The type of requirement: permission, obligation, etc.
- The requirement pattern
- The traceability information (requirement ID, line number and paragraph index)



Requirement Specification – 2

Requirement Body

Slot	Value
subject Logical-AND Logical-OR	A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO *A group health plan that creates or receives* protected health information in addition to summary health information as defined in §164.504(a) *A group health plan that creates or receives* information on …
act	*must…* provide
object	a notice under this section
target	*to…* any person



Envisioned Use and Future Work

- Consistency checking for frame-based models
- Future integration with:
  - ❑ Goal-oriented Requirements Analysis
  - ❑ Business Process Modeling
  - ❑ Model-Driven Architecture
- A product for coordinating relevant changes to law
- A product for focusing risk analysis