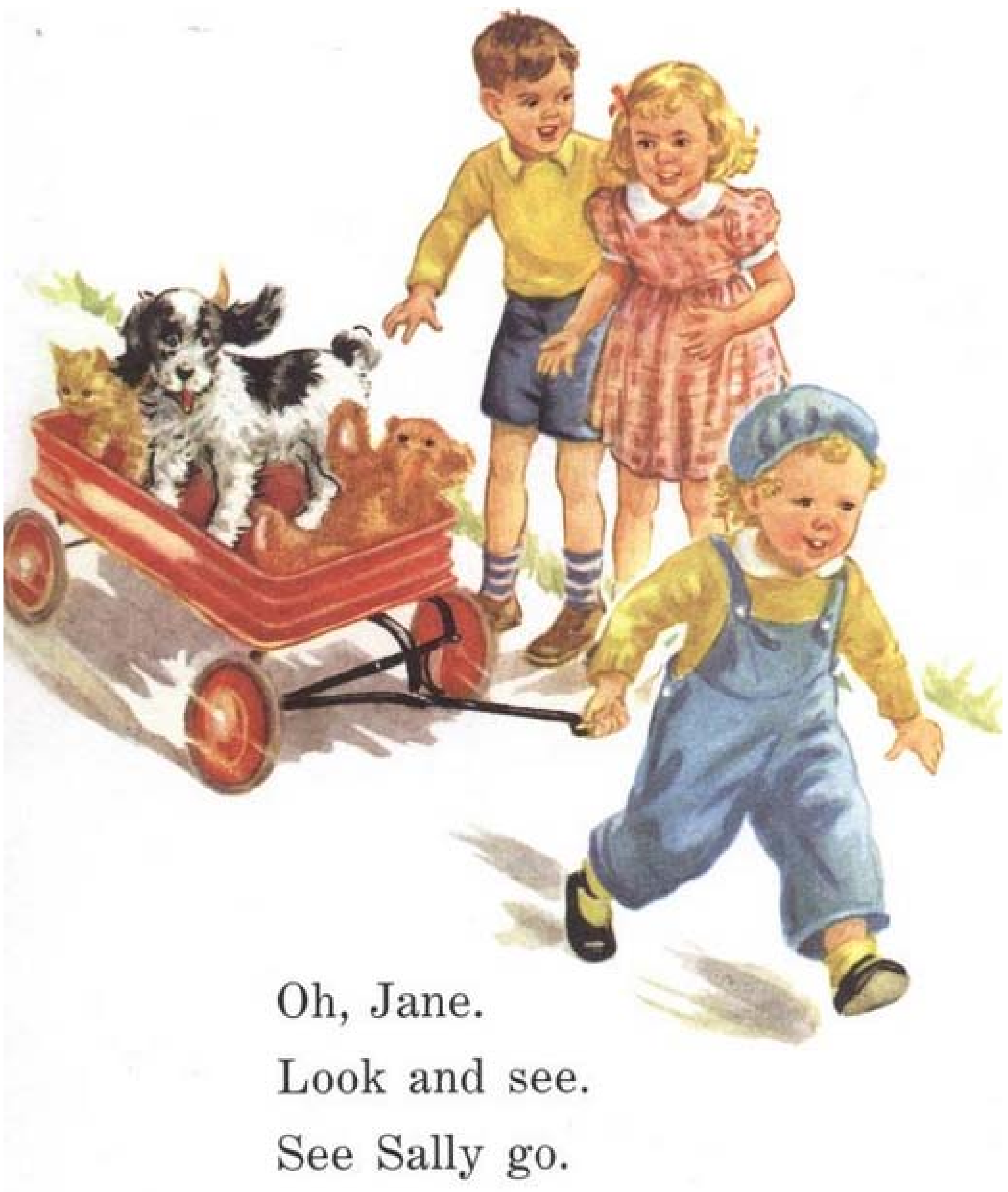
Thinking with pictures
Building with words

A Business Rules Primer from XpressRules® LLC



Oh, Jane.
Look and see.
See Sally go.

Oh, Meixiu.

See Heidi use XpressRules.

See her produce authoring screens and business rules and access policies and computer code and audit records.

See Heidi help Operations reduce Risk Management's total cost of info access control by 38%.

So how does Heidi do all that?

This is the Risk Management Group.

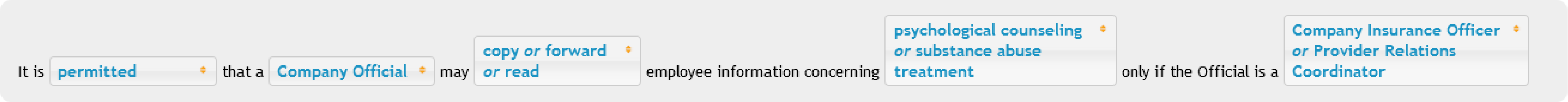
They protect the company's information assets.

They are not programmers.

They write business rules.

Business rules are sentences.

Some business rules are access rules. An access rule restricts who may see specific information:



It is permitted that a Company Official may copy *or* forward *or* read employee information concerning psychological counseling *or* substance abuse treatment only if the Official is a Company Insurance Officer *or* Provider Relations Coordinator

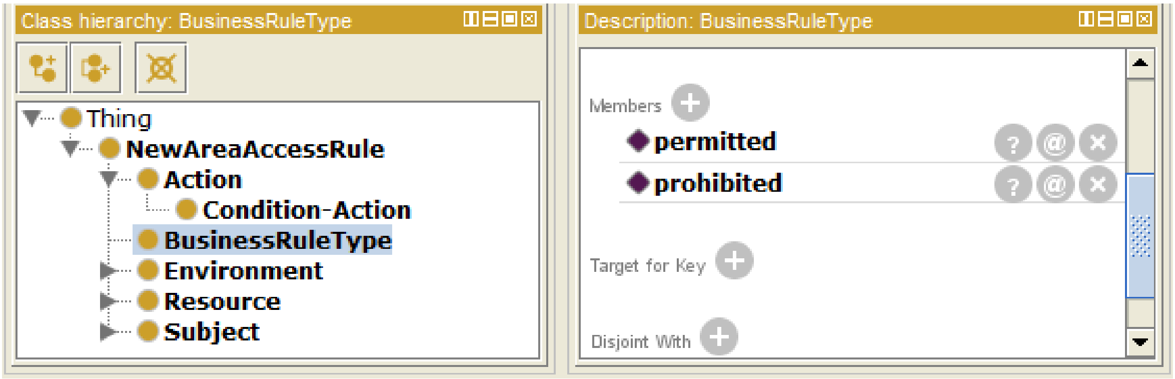
This is Heidi.

Heidi is an intern.

She helps the Risk Management Group.

Heidi uses XpressRules. She is an accurate typist. She is not a programmer.

She types the RMG's description of the rule's sentence layout.



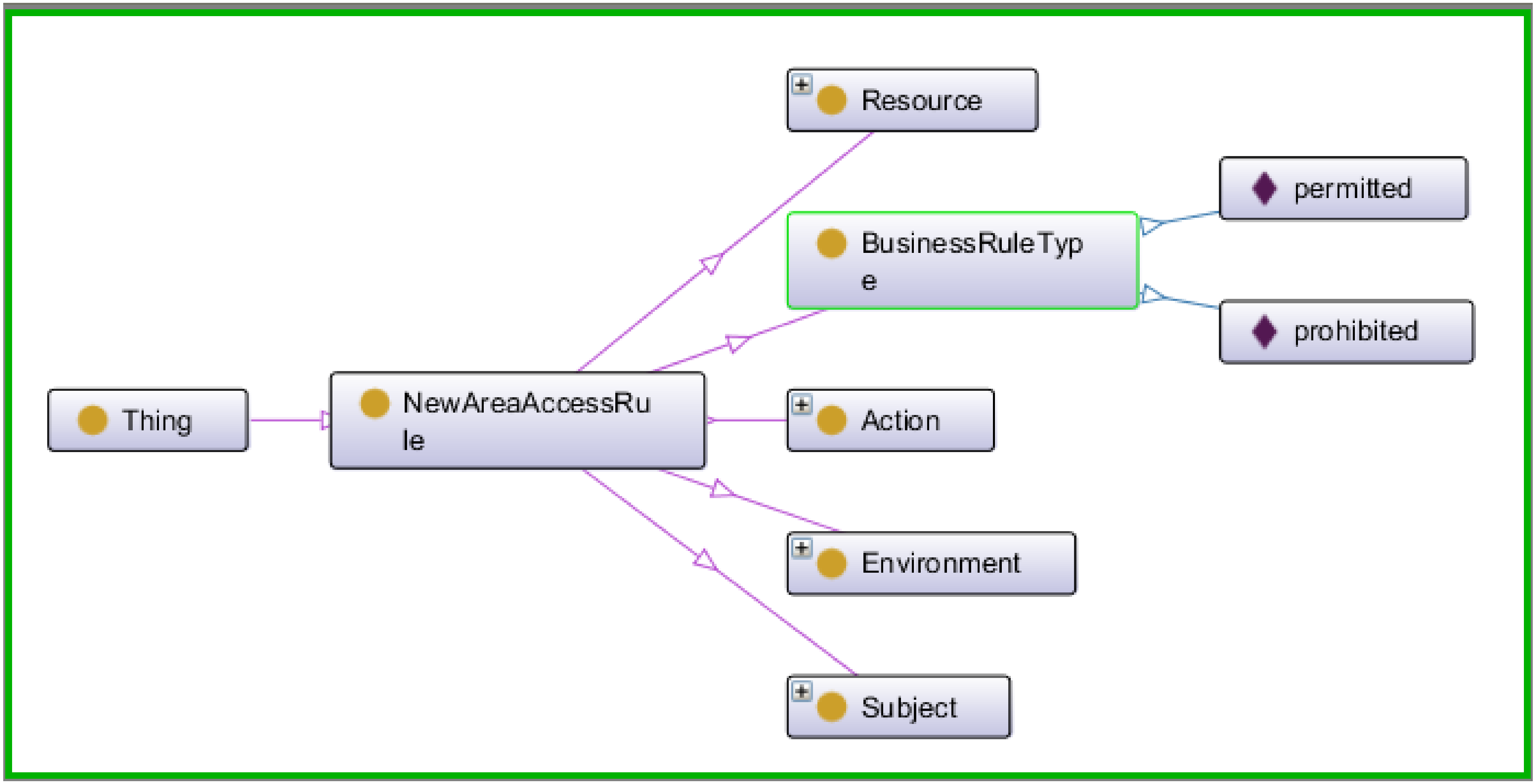
Class hierarchy: BusinessRuleType

- Thing
  - NewAreaAccessRule
    - Action
      - Condition-Action
    - BusinessRuleType
    - Environment
    - Resource
    - Subject

Description: BusinessRuleType

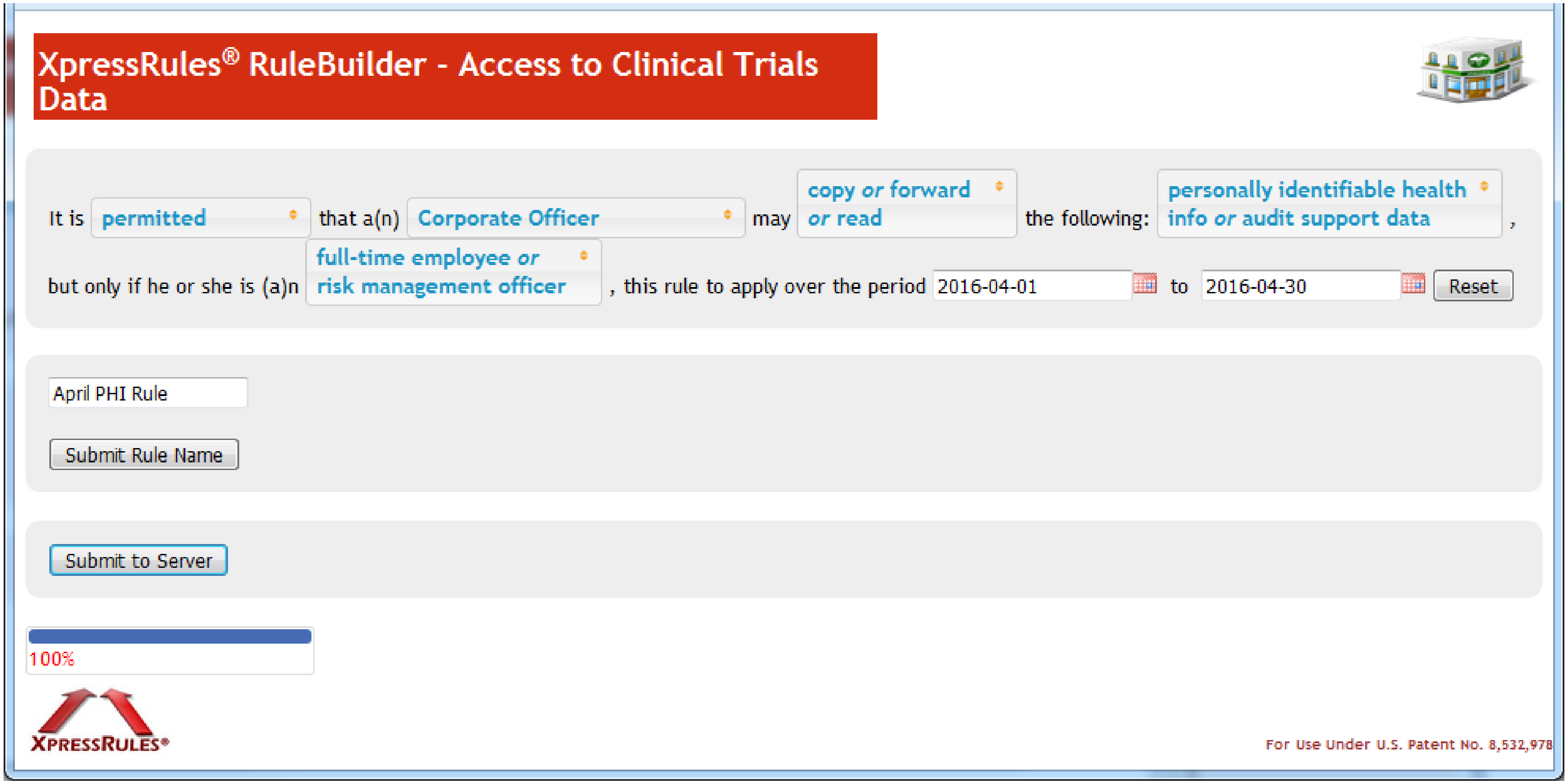
Members
- permitted
- prohibited

Her words create a picture of the sentence’s layout:



The RMG requires a rule authoring console.

XpressRules creates the rule authoring console:



XpressRules® RuleBuilder - Access to Clinical Trials Data

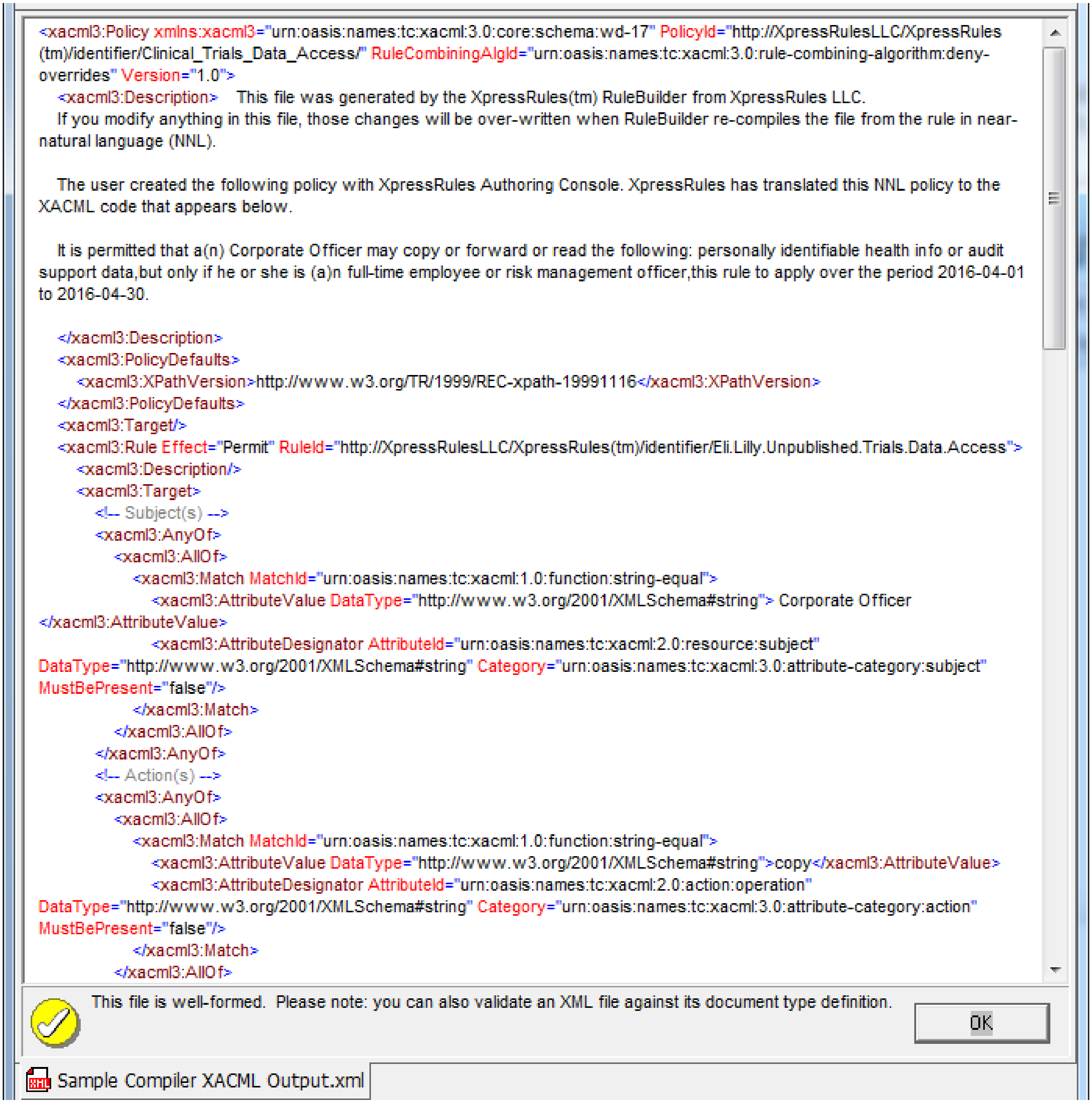
It is permitted that a(n) Corporate Officer may copy *or* forward *or* read the following: personally identifiable health info *or* audit support data, but only if he or she is (a)n full-time employee *or* risk management officer, this rule to apply over the period 2016-04-01 to 2016-04-30

April PHI Rule

100%

For Use Under U.S. Patent No. 8,532,978

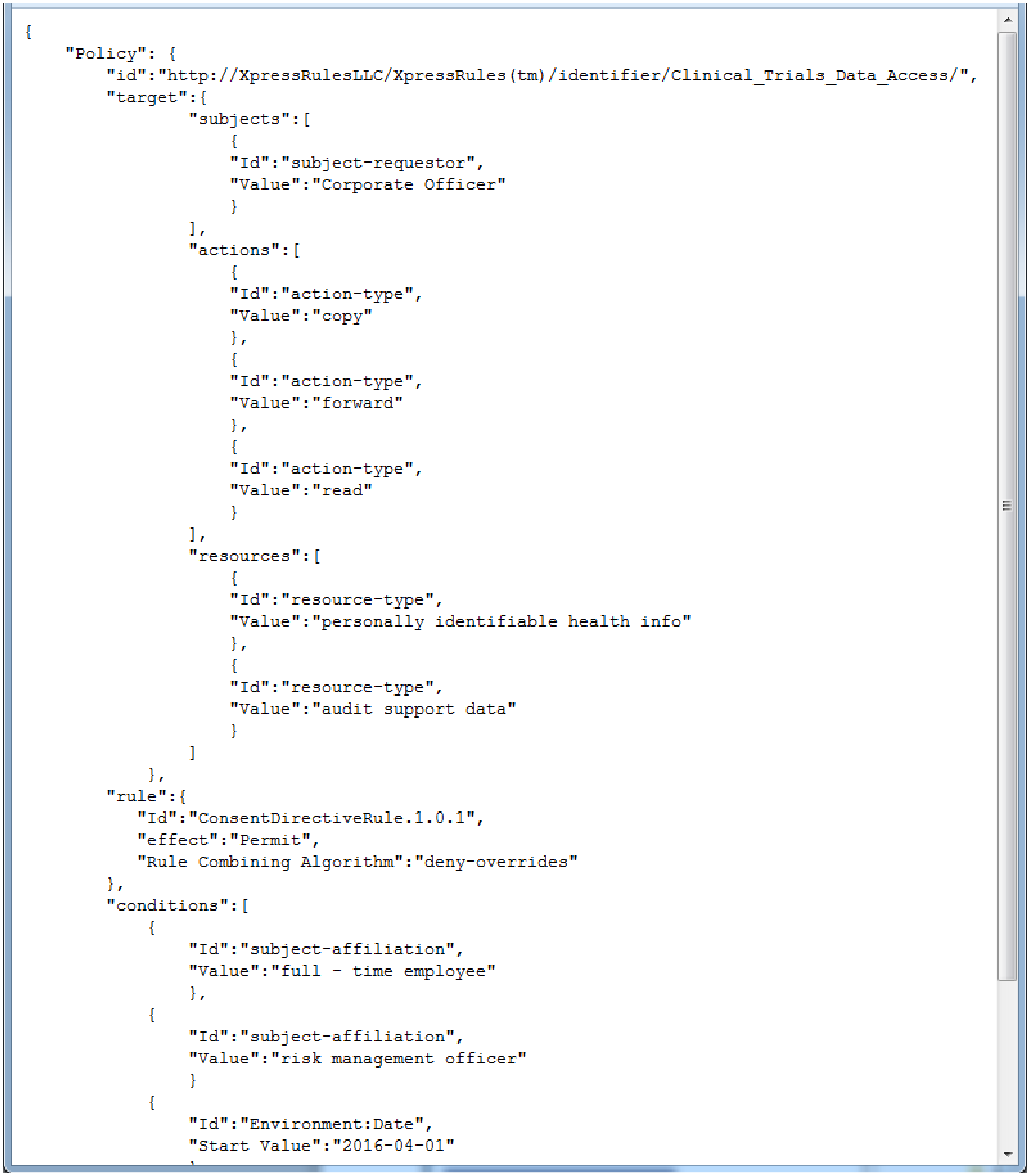
The company’s security server requires computer code. XpressRules creates the rules’ computer code as XACML 3.0:



```
<xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="http://XpressRulesLLC/XpressRules
(tm)/identifier/Clinical_Trials_Data_Access/" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-
overrides" Version="1.0">
  <xacml3:Description>   This file was generated by the XpressRules(tm) RuleBuilder from XpressRules LLC.
  If you modify anything in this file, those changes will be over-written when RuleBuilder re-compiles the file from the rule in near-
natural language (NNL).

  The user created the following policy with XpressRules Authoring Console. XpressRules has translated this NNL policy to the
XACML code that appears below.

  It is permitted that a(n) Corporate Officer may copy or forward or read the following: personally identifiable health info or audit
support data,but only if he or she is (a)n full-time employee or risk management officer,this rule to apply over the period 2016-04-01
to 2016-04-30.

  </xacml3:Description>
  <xacml3:PolicyDefaults>
    <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:XPathVersion>
  </xacml3:PolicyDefaults>
  <xacml3:Target/>
  <xacml3:Rule Effect="Permit" RuleId="http://XpressRulesLLC/XpressRules(tm)/identifier/Eli.Lilly.Unpublished.Trials.Data.Access">
    <xacml3:Description/>
    <xacml3:Target>
      <!-- Subject(s) -->
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> Corporate Officer
</xacml3:AttributeValue>
            <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:resource:subject"
DataType="http://www.w3.org/2001/XMLSchema#string" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
MustBePresent="false"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
      <!-- Action(s) -->
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">copy</xacml3:AttributeValue>
            <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:action:operation"
DataType="http://www.w3.org/2001/XMLSchema#string" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
MustBePresent="false"/>
          </xacml3:Match>
        </xacml3:AllOf>
```

This file is well-formed. Please note: you can also validate an XML file against its document type definition.

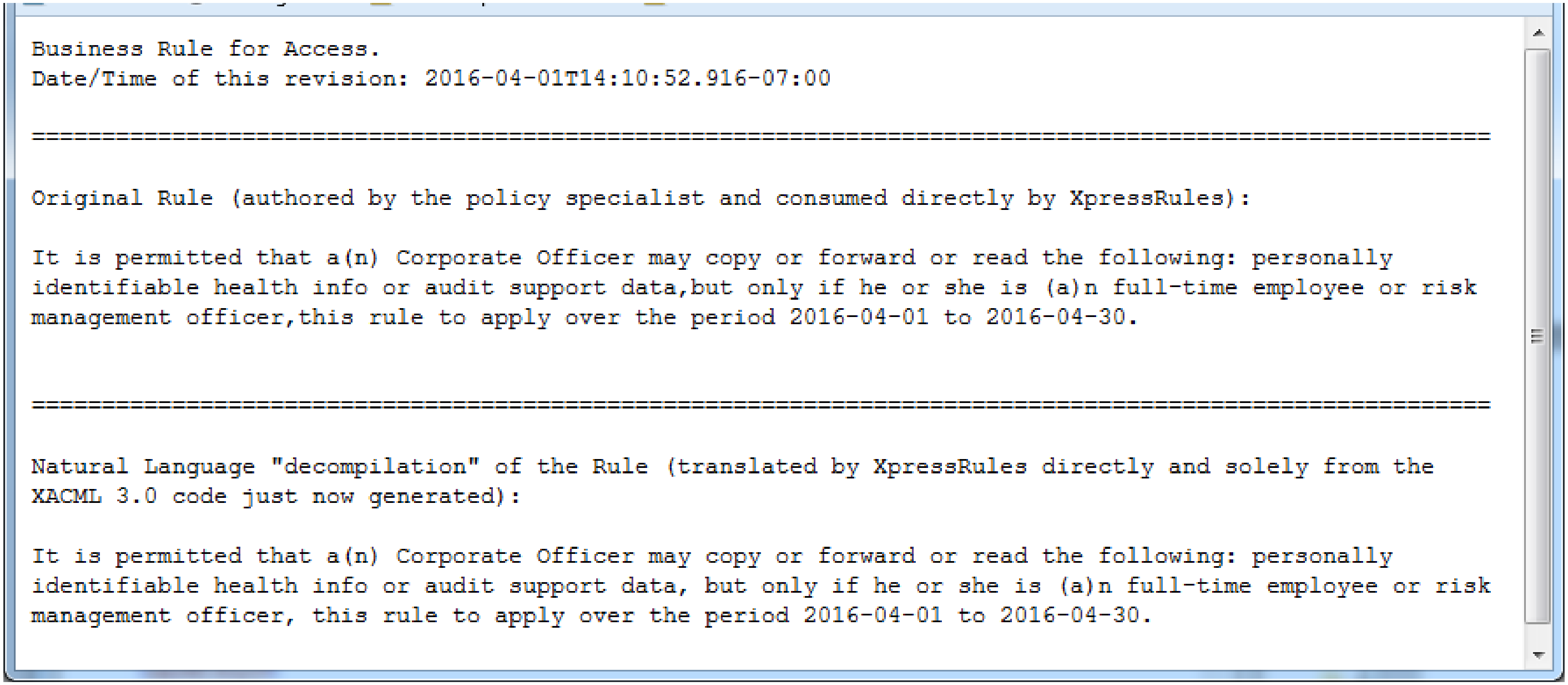
The Company's IT Department prefers JSON. XpressRules also creates the rules' computer code as JSON:



```
{
    "Policy": {
        "id":"http://XpressRulesLLC/XpressRules(tm)/identifier/Clinical_Trials_Data_Access/",
        "target":{
                "subjects":[
                    {
                    "Id":"subject-requestor",
                    "Value":"Corporate Officer"
                    }
                ],
                "actions":[
                    {
                    "Id":"action-type",
                    "Value":"copy"
                    },
                    {
                    "Id":"action-type",
                    "Value":"forward"
                    },
                    {
                    "Id":"action-type",
                    "Value":"read"
                    }
                ],
                "resources":[
                    {
                    "Id":"resource-type",
                    "Value":"personally identifiable health info"
                    },
                    {
                    "Id":"resource-type",
                    "Value":"audit support data"
                    }
                ]
            },
        "rule":{
           "Id":"ConsentDirectiveRule.1.0.1",
           "effect":"Permit",
           "Rule Combining Algorithm":"deny-overrides"
        },
        "conditions":[
            {
                "Id":"subject-affiliation",
                "Value":"full - time employee"
                },
            {
                "Id":"subject-affiliation",
                "Value":"risk management officer"
                }
            {
                "Id":"Environment:Date",
                "Start Value":"2016-04-01"
```

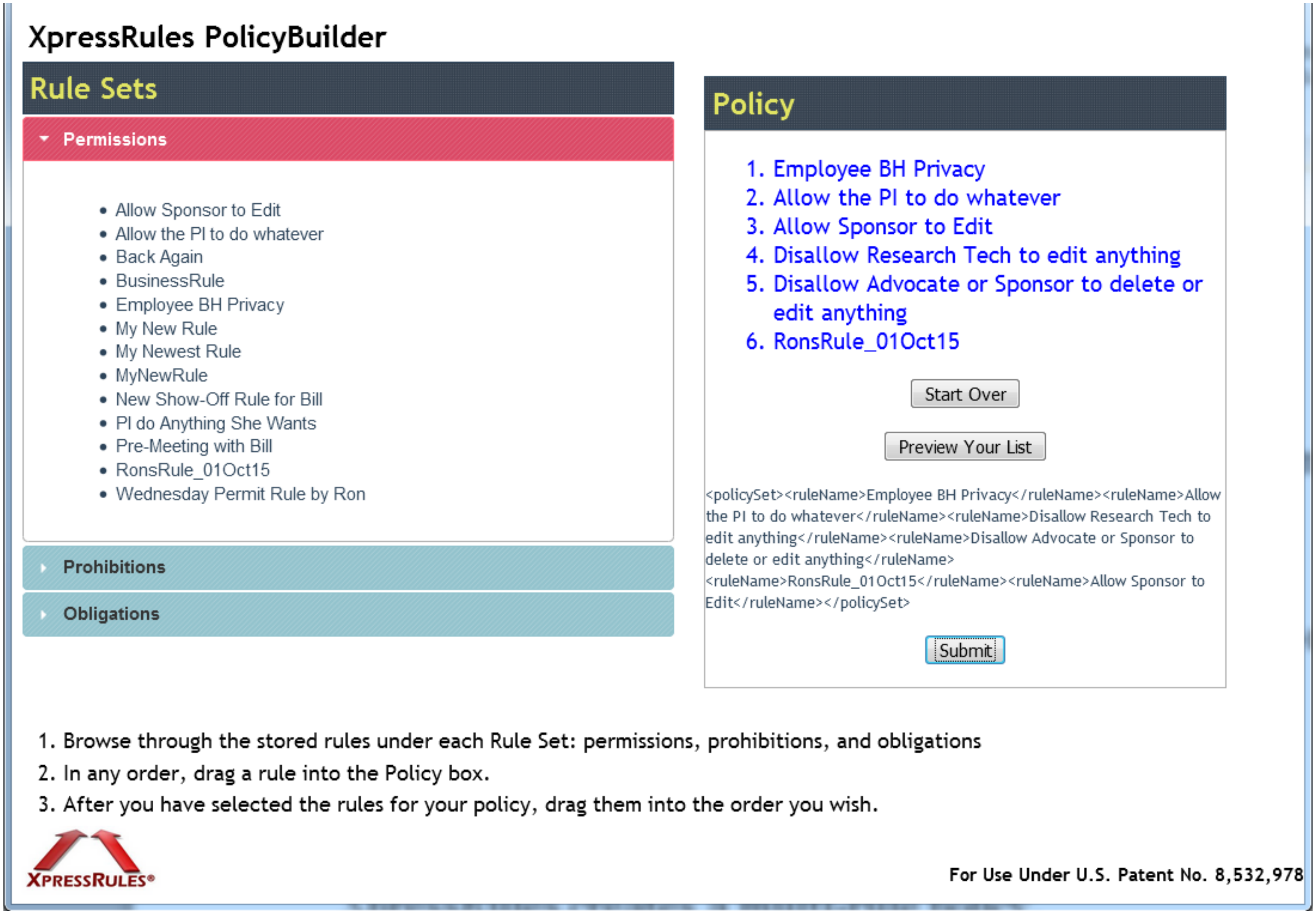
The company’s audit team requires readable histories.

XpressRules creates an auditors’ “Round Trip” (NNL→Code→NNL) for each rule:



```
Business Rule for Access.
Date/Time of this revision: 2016-04-01T14:10:52.916-07:00

==============================================================================

Original Rule (authored by the policy specialist and consumed directly by XpressRules):

It is permitted that a(n) Corporate Officer may copy or forward or read the following: personally
identifiable health info or audit support data,but only if he or she is (a)n full-time employee or risk
management officer,this rule to apply over the period 2016-04-01 to 2016-04-30.


==============================================================================

Natural Language "decompilation" of the Rule (translated by XpressRules directly and solely from the
XACML 3.0 code just now generated):

It is permitted that a(n) Corporate Officer may copy or forward or read the following: personally
identifiable health info or audit support data, but only if he or she is (a)n full-time employee or risk
management officer, this rule to apply over the period 2016-04-01 to 2016-04-30.
```

The RMG requires complex (multi-rule) policies. They select their pre-stored rules with XpressRules' Policy Builder:



- Allow Sponsor to Edit
- Allow the PI to do whatever
- Back Again
- BusinessRule
- Employee BH Privacy
- My New Rule
- My Newest Rule
- MyNewRule
- New Show-Off Rule for Bill
- PI do Anything She Wants
- Pre-Meeting with Bill
- RonsRule_01Oct15
- Wednesday Permit Rule by Ron

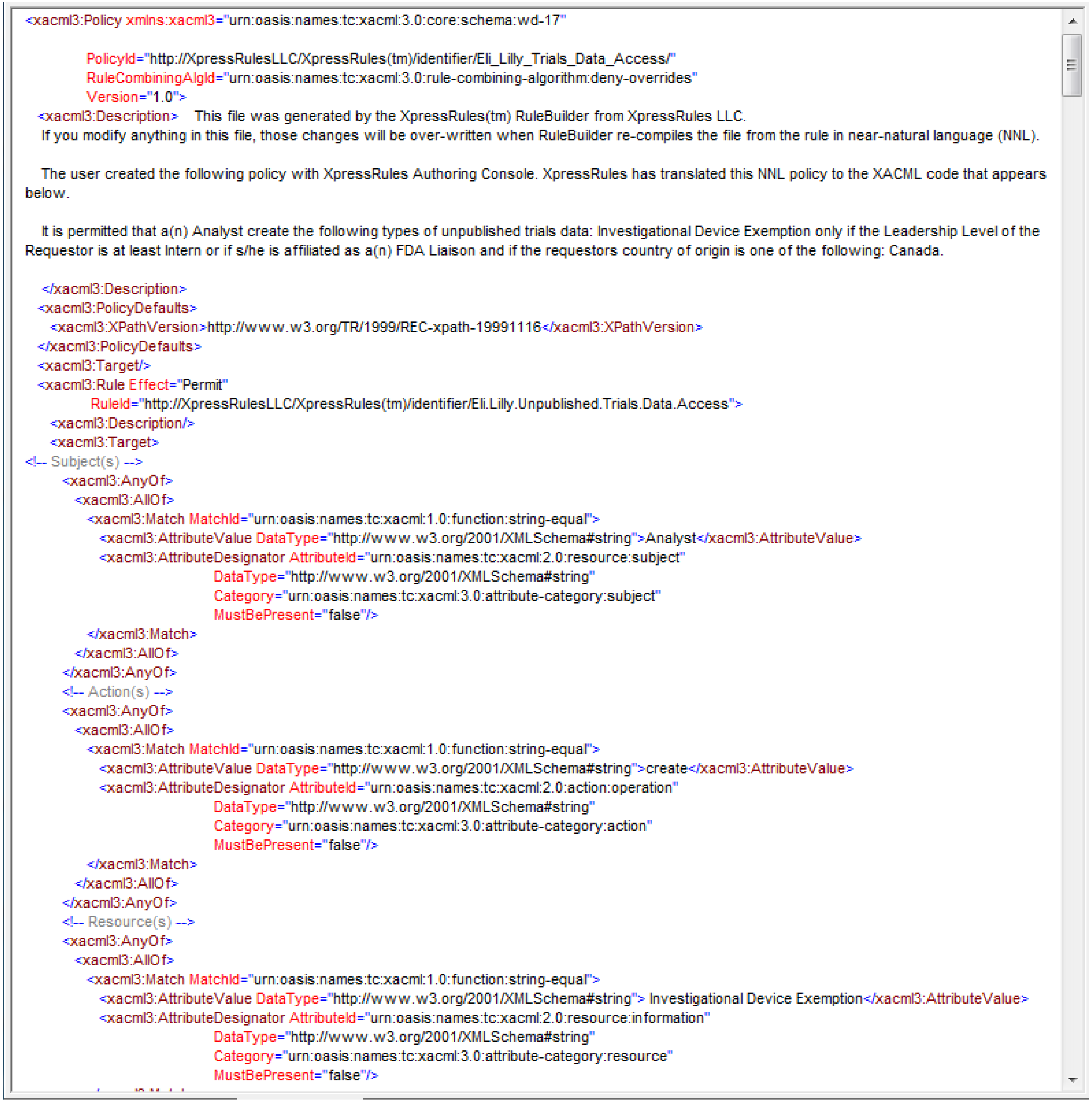
1. Employee BH Privacy
2. Allow the PI to do whatever
3. Allow Sponsor to Edit
4. Disallow Research Tech to edit anything
5. Disallow Advocate or Sponsor to delete or edit anything
6. RonsRule_01Oct15

```
<policySet><ruleName>Employee BH Privacy</ruleName><ruleName>Allow
the PI to do whatever</ruleName><ruleName>Disallow Research Tech to
edit anything</ruleName><ruleName>Disallow Advocate or Sponsor to
delete or edit anything</ruleName>
<ruleName>RonsRule_01Oct15</ruleName><ruleName>Allow Sponsor to
Edit</ruleName></policySet>
```

1. Browse through the stored rules under each Rule Set: permissions, prohibitions, and obligations
2. In any order, drag a rule into the Policy box.
3. After you have selected the rules for your policy, drag them into the order you wish.

For Use Under U.S. Patent No. 8,532,978

XpressRules creates the multi-rule policy (858 total lines of XACML code):



```
<xacml3:Policy xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"

          PolicyId="http://XpressRulesLLC/XpressRules(tm)/identifier/Eli_Lilly_Trials_Data_Access/"
          RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides"
          Version="1.0">
  <xacml3:Description>    This file was generated by the XpressRules(tm) RuleBuilder from XpressRules LLC.
   If you modify anything in this file, those changes will be over-written when RuleBuilder re-compiles the file from the rule in near-natural language (NNL).

   The user created the following policy with XpressRules Authoring Console. XpressRules has translated this NNL policy to the XACML code that appears
below.

   It is permitted that a(n) Analyst create the following types of unpublished trials data: Investigational Device Exemption only if the Leadership Level of the
Requestor is at least Intern or if s/he is affiliated as a(n) FDA Liaison and if the requestors country of origin is one of the following: Canada.

   </xacml3:Description>
  <xacml3:PolicyDefaults>
    <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:XPathVersion>
  </xacml3:PolicyDefaults>
  <xacml3:Target/>
  <xacml3:Rule Effect="Permit"
          RuleId="http://XpressRulesLLC/XpressRules(tm)/identifier/Eli.Lilly.Unpublished.Trials.Data.Access">
    <xacml3:Description/>
    <xacml3:Target>
<!-- Subject(s) -->
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Analyst</xacml3:AttributeValue>
            <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:resource:subject"
                                  DataType="http://www.w3.org/2001/XMLSchema#string"
                                  Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
                                  MustBePresent="false"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
      <!-- Action(s) -->
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">create</xacml3:AttributeValue>
            <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:action:operation"
                                  DataType="http://www.w3.org/2001/XMLSchema#string"
                                  Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                  MustBePresent="false"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
      <!-- Resource(s) -->
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> Investigational Device Exemption</xacml3:AttributeValue>
            <xacml3:AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:resource:information"
                                  DataType="http://www.w3.org/2001/XMLSchema#string"
                                  Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                                  MustBePresent="false"/>
```

The company’s CFO says, “Well done, RMG. You have reduced our annual TCO for info asset protection by 38%!”

The RMG says, “Good work, Heidi! Come back after graduation.”

So how *does* Heidi and the RMG do all this?

Thinking with pictures. . .

The RMG designs a small number of sentence layouts, which will support thousands of possible company-specific rules:

Building with words

The RMG supplies the vocabulary for the rules.

Heidi takes (1) the RMG's layout and vocabulary and (2) uses a free modeling tool to describe the sentence layout. When she presses SAVE , XpressRules. . .

Finishes the Picture

XpressRules uses Heidi's saved picture to create:

- The RuleBuilder Authoring Console
- The PolicyBuilder Console
- XACML 3.0 computer code for every rule created at the Authoring Console
- XACML 3.0 multi-rule policies
- JSON computer code for every rule
- The rule's "Round-Trip" integrity report for the auditor

About “sentence layout”:

If the language of pages 3-13 feels a bit “constrained,” it is. And here’s why. Besides the Dick-and-Jane font, each sentence on every page is squeezed into one of two simple “layouts,” each with three parts:

1.

Subject	Action	Something
Heidi	uses	XpressRules.
The company’s audit team	requires	readable histories.
The company’s CFO	says	“Well done…”

2.

Subject	Form of “be”	Something
Hedi	is	an intern.
Business rules	are	sentences.
She	is not	a programmer.

Business Rules are constrained as well. An XpressRules’ BR always begins with one of the following Rule Types:

- It is permitted that…
- It is prohibited that…
- It is obligatory that….

The “layout” of an XpressRules’ access policy—a type of Business Rule—typically looks like Heidi’s console (p. 6):

Rule Type	Subject	Action	Resource	Condition(s)
It is permitted that	a Company Official	may copy…	information…	only if …

Using just simple-sentence rules like the one on page 6, non-IT policy authors (and their assistants) can create very complex multi-rule policies. These policies will support most of the cases required by an entire organization.