



XACML 2.0 RSA 2008 Interop Scenarios WALK THROUGH - Version 0.7

Working Draft

5 April 2008

Notices

Copyright © OASIS® 1993–2008. All Rights Reserved. OASIS trademark, IPR and other policies apply.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names and abbreviations here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

1 Introduction

This document provides a guide for both testing and demonstrating the XACML healthcare application at the 2008 RSA Conference. The focus of the document will be on the individual steps that comprise each use case in the Interop document “XACML 2.0 RSA 2008 Interop Scenarios.”

The use cases described below fall into five general categories: enterprise permissions, consent directives, security business rules, emergency access, and data filtering based on patient election.

1.1 Initial Steps

The use cases are accessed through a web browser from any system that is jacked into the switch at the XACML booth on the RSA floor. Interactions with the provided medical application discussed below will allow participants to exercise the use case in the Interop.

1.2 Notes on Provider Names

The Interop use cases include steps that set or clear permissions and constraints. Therefore a login representing the clinician (provider) has been created for each participant. The naming convention that must be followed is shown below:

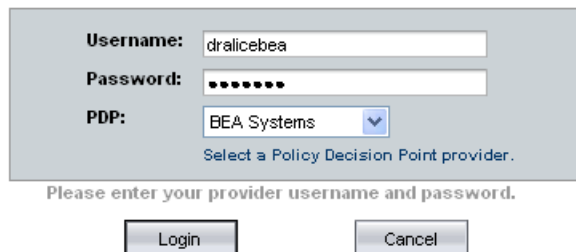
```
username in form: drbob<vendorname all lower case>
e.g. username: drbobibm
password: rsa2008
```

When testing or demonstrating the use cases in the Interop document, each participant should use the actor's name (e.g. Dr. Bob) with the company suffix. The resulting provider username is all lower case with no spaces. The passwords for all user IDs are the same. During your demonstration of the use cases below, you may want to have two instances of your browser displayed; one for the provider, one for the security administrator. Two browser instances will allow you to change permissions or constraints without logging off as the provider.

2. Demonstrating the Use Cases

2.1 Login to the Application

Login in to the application using the provider username. As described in section 1.2, each participant has their own set of clinician user IDs. The password is “rsa2008” for all providers. Because the provider properties are changed during the demonstration, usernames vary between the use cases. The example below is appropriate for the use case demonstration HL7 permissions.



Username: dralicebea

Password: rsa2008

PDP: BEA Systems

Select a Policy Decision Point provider.

Please enter your provider username and password.

Login Cancel

Figure 1: Example login for Dr. Alice by participant BEA

2.1.1 HL7 Role/Permissions

The purpose of this use case is to demonstrate that XACML can be used to express and enforce the enterprise-wide permissions that are used in a role based access control environment. Permissions will be distinguished from patient consent directives and business rules in later use cases.

After logging into the application as Dr. Alice (cf. Figure 1), you must select a patient. Since patient constraints can be added or removed using the application, participants will be provided a pool of patient names for their individual use. For this version of the Guide, we will search on “Smith” and choose a random patient.

Lastname	<input type="text" value="smith"/>	Firstname	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>
----------	------------------------------------	-----------	----------------------	---------------------------------------	--------------------------------------

Note: Patient must be selected before continuing.

MPI	name	gender	Date of Birth	Address
160379	SMITH,ANNA	F	Mon May 07 14:57:46 PST 1934	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
462474	SMITH,ANNA	F	Tue Mar 17 14:57:46 PST 1970	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
545591	SMITH,ANNA	F	Tue Feb 23 14:57:46 PST 1999	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
412272	SMITH,BAMBI	F	Wed Jun 25 14:57:46 PDT 1952	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
606505	SMITH,ELLIOT	M	Tue Jul 31 14:57:46 PDT 1979	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345

Figure 2: Selecting a patient

The providers have been populated with all the permissions required to view patient information. After a patient has been selected use the “chart” link on the left navigation bar to attempt to view patient data. With the initial permissions granted to all providers, you should be able to view a patient record similar to the screen shown in Figure 3.

PDP Provided By:	Sun Microsystems	Doctor, Alice S	Facility A
------------------	------------------	-----------------	------------

Patient Info

Name

Facility

Gender

☐ Male ☒ Female

DoB

Chart Cover Sheet

Active Problems & Diagnosis

ICD9	Desc.	Onset
No Results Found		

Active/Recent Medications

Med Name	Dosage	Fill Date	HDC
CALCIUM CARBONATE (OSCAL)--PO 500MG TAB	null	Mar 22, 2004	00536-4106-08
LISINOPRIL (ZESTRIL)--PO 5MG TAB	null	Feb 16, 2004	00143-1266-10
CLINDAMYCIN (CLEOCIN)--PO 150MG CAP	null	Feb 14, 2004	00591-5708-01
ASPIRIN (BABY)--PO 81MG TBCH	null	Feb 3, 2004	00904-4040-73

Allergies

Type/Name	Date Noted
No results found	

Figure 3: Accessing the medical record of a patient

Later in the demonstration, the participants will change the permissions held by Dr. Alice by logging into the application as the security administrator. Keep a second browser session going and return as the

security administrator after each demonstration to restore the permissions held by Dr. Alice. If you do not see the medical record, you probably need to restore the permissions held by the user account.

Prior to changing the permissions held by Dr. Alice, the participants may want to show the retrieval of the provider's permissions stored in the PIP. Use the "View PIP Interactions" link on the left navigation bar, as shown in Figure 4.

The screenshot shows a web application interface. On the left is a navigation bar with the following items: Patient Search, View PDP Interaction, **View PIP Interactions** (highlighted with a red circle), Logoff, Interop Tools, Patient Elections, User Based Access, Masked Access, Provider Permissions, Obligation Management, and Data Filtering. The main content area on the right is titled 'End PEP/PIP Interactions' and contains a log of interactions:

```

Begin PEP/PIP Request Initialization
PIP Request: Tue Apr 01 16:03:25 PDT 2008 getPdpEntity(BEA Systems,http://localhost/PolicyDecisionPoint/PDPService?WSDL)
PIP Response: Tue Apr 01 16:03:25 PDT 2008 beaPdpEntity
PIP Request: Tue Apr 01 16:03:25 PDT 2008 getProviderInfo
(dralicebea,http://localhost/PermissionServices/HL7PermissionCodesService?WSDL)
PIP Response: Tue Apr 01 16:03:25 PDT 2008 providerName: Doctor, Alice B, facilityId: Facility A
PIP Request: Tue Apr 01 16:03:25 PDT 2008 getProviderRoles(100008,
http://localhost/PermissionServices/HL7PermissionCodesService?WSDL)
PIP Response: Tue Apr 01 16:03:25 PDT 2008 providerRoles: physician
PIP Request: Tue Apr 01 16:03:25 PDT 2008 getProviderPermissions(100008,
http://localhost/PermissionServices/HL7PermissionCodesService?WSDL)
PIP Response: Tue Apr 01 16:03:25 PDT 2008 providerPermissions:
PRD-003
PRD-005
PRD-006
PRD-009
PRD-010
PRD-012
PRD-017
PIP Request: Tue Apr 01 16:03:25 PDT 2008 getPatientDirectives(412272, http://localhost/DirectiveServices/PatientDirectiveService?
WSDL)
PIP Response: Tue Apr 01 16:03:25 PDT 2008 patientConsentDirective: N
PIP Request: Tue Apr 01 16:03:25 PDT 2008 getSensitiveDataFilteringRequirements(medical-record,
http://localhost/SensitiveDataAndFilteringServices/DataAttributeService?WSDL)
PIP Response: Tue Apr 01 16:03:25 PDT 2008 sensitiveAttributes:
End PEP/PIP Interactions
  
```

Figure 4: Showing the retrieval of HL7 permissions

The application allows the participants to show guests the HL7 permissions retrieved from the PIP and passed between the PEP and PDP. Use the "View PDP Interactions" link on the left navigation bar, to show the exchange of permissions in the XACML context. At this point Dr. Alice will be presenting all the required permissions to the PDP.

We will remove the permissions assigned to Dr. Alice to demonstrate the permissions are being evaluated by the XACML policy engine. In a second browser instance, login as the security administrator "securityadmin," as shown in figure 5. You must specify a PDP. Keeping two windows up will speed up presentation of the demonstration, since you must use the securityadmin user to change permissions and constraints to perform the use cases below. Using two browser windows will also allow you to display interactions between the PEP and PDP while making access calls on the other session.

The screenshot shows a login form with the following fields and controls:

- Username:** A text input field containing "securityadmin".
- Password:** A text input field with masked characters (dots).
- PDP:** A dropdown menu currently showing "BEA Systems".
- Below the PDP dropdown is a link: "Select a Policy Decision Point provider."
- Below the form is a prompt: "Please enter your provider username and password."
- At the bottom are two buttons: "Login" and "Cancel".

Figure 5: Logging in as the security administrator

The security administrator has been granted permissions required to change the permissions on providers (SEC-001) and search on patient name (PRD-006). Once logged in as the security

administrator, participants may want to display these permissions in the XACML context using the “View PDP Interactions” link on the left navigation bar.

As the security administrator “Security, Bob,” select the “Provider Permissions” link beneath the “Interop Tools” on the left navigation bar. A screen similar to Figure 6 will appear, select the Dr. Alice with the initial appropriate to the participant (in this case Sun Microsystems).

Figure 6: Specifying the Dr. Alice for removing permissions

The application will populate the grayed-out fields specific to the chosen provider. Now select the role possessed by Dr. Alice and click on “Remove Selected Role From Provider” as shown in Figure 7. The application will refresh and the role previously held by Dr. Alice should be missing.

Figure 7: Removing permissions of Dr. Alice

Without the role of physician, Dr. Alice no longer has the collection of permissions previously asserted. Use the browser displaying the session Dr. Alice logged into to demonstrate the effect of removing the permissions. Select “chart” to attempt access to the medical record. The request will fail and the “Emergency Override” screen will appear. Do not select an override because you do not have the permission to declare and emergency. Use the “View PDP Interactions” on the left navigation bar to show how the subject has no permissions therefore the PDP returns a deny.

Return to the browser displaying the security administrator's session and restore the physician role to Dr. Alice by highlighting the physician role in the lower pull down menu and select "Add Selected Role To Provider." Dr. Alice will now be able to view the chart and the permissions will again be seen for the subject in the PDP interaction screen.

2.1.2 HL7 Patient Consent Directives

The purpose of this use case is to demonstrate that XACML can be used to express and enforce patient consent directives. Obviously, patients do not have the ability to change the assignment of enterprise-wide permissions held by providers. However, patients can constrain the use of permissions held by the provider when viewing the patient's medical information. Fine grain control is demonstrated in a later use case by masking an individual region of the medical record.

For this demonstration, the security administrator will add the elections made by the patient. This simplifies the demonstration application. Typically, a portal would be used to allow the patient to directly control access to their medical records.

Begin the use case by logging into the application as Dr. Bob as shown in Figure 8. Use the suffix and PDP appropriate to the participant.

Username:

Password:

PDP:

[Select a Policy Decision Point provider.](#)

Please enter your provider username and password.

Figure 8: Logging in as Dr. Bob

Initially, patients have no constraint directives stored. Since patient constraints can be added or removed using the application, participants will be provided a pool of patient names for their individual use. For this version of the Guide, we will search on "Smith" and choose a random patient. Remember to remove any constraints set by the patient before demonstrating this use case using the same patient name.

After a patient has been selected use the "chart" link on the left navigation bar to attempt to view patient data. With the initial permissions, you should be able to view a patient record similar to the screen shown in Figure 3 will be displayed.

We will now store a patient directive that removes Dr. Bob's ability to view the medical record of the selected patient. The HL7 consent code UBA (user based access) represents a complete bar of a specified requestor or role to the specified subject's medical record. To set the UBA, start a second browser instance, if you have not already, and use it log in as the security administrator, as shown in Figure 5. You must specify a PDP.

After logging into the application as the security administrator, select the patient previously demonstrated. As discussed above, the security administrator possesses the SEC-001 privilege, therefore can set consent directives on behalf of the patient. To demonstrate a complete bar use the "User Based Access" link under "Patient Elections" beneath the "Interop Tools" on the left navigation bar.

As shown in Figure 9, you will see a list of all patient consent directives. You may have to hit the reset button to ensure the initial value of the security administrator is cleared. You may now use the pull down menu to select the provider you wish to block for the patient you previously selected. The provider assigned to BEA is selected in the Figure, denoted by the initial "B" in the selection.

The screenshot shows a web application interface. On the left is a sidebar with navigation links: Info, Problem List, Procedures, Laboratory, Radiology, Medications, Tests, DP Interaction, and IP Interactions. The main area is titled "Current Providers with Access" and features a dropdown menu for selecting a provider. The dropdown menu is open, showing a list of providers: Doctor, Charlie A, Doctor, Bob B (highlighted), Doctor, Alice B, Doctor, Charlie B, Doctor, Bob C, Doctor, Alice C, Doctor, Charlie C, Doctor, Bob I, Doctor, Alice I, Doctor, Charlie I, Doctor, Bob O, Doctor, Alice O, Doctor, Charlie O, Doctor, Bob O, Doctor, Alice O, Doctor, Charlie O, Doctor, Bob R, Doctor, Alice R, Doctor, Charlie R, Doctor, Bob S, Doctor, Alice S, and Doctor, Charlie S. Below the dropdown menu, the "Provider Name" is set to "Doctor, Bob B". To the right of the dropdown menu, there are fields for "Facility" (set to "Facility A") and "Provider Identifier" (set to "100004"). Below these fields are three buttons: "Add Constraint", "Remove Constraint", and "Reset".

providerID	providerName	facilityID
100004	Doctor, Bob A	Facility A
		Facility A

Click on "providerID" field to select provider.

Figure 9: Selecting Dr. Bob for a BEA demonstration on consent directives

Note that each participant should select the provider, Dr. Bob, with the initial corresponding to the participant. Since the screen capture in Figure 9 was for the BEA case, we selected Doctor, Bob B.

After making your selection, check that the shaded text areas have been correctly populated with the expected provider information. You can use the reset button to clear the loaded data if necessary.

Select the "add constraint" button. The screen will refresh, showing a UBA consent directive on behalf of the selected patient against the selected provider, e.g. Dr. Bob B in the example above.

Return to the browser instance that you used to login as Dr. Bob. Perform the patient search to return to the patient upon whose behalf the UBA consent directive was just made. Or if you prefer to use one browser window, log out of the security administrator session and log back in as Dr. Bob.

Remove the constraint by returning as the security admin to the screen in Figure 9. Then select the patient name and provided name previously demonstrated. After making this selection, check that the shaded text areas have been correctly populated with the expected provider information. You can use the reset button to clear the loaded data.

Select the "Remove Constraint" button. The screen will refresh, showing the UBA consent directive on behalf of the selected patient against the selected provider has been removed.

2.1.3 Security Business Rule

The purpose of this use case is to demonstrate that XACML can be used to enforce an enterprise business rule. Business rules arise when enterprise governance mandates a certain application behavior that can not be translated easily into the permissions held by the actor. For example, in this use case the business rule requires that a clinical progress note detailing the medical state and suggested treatment of a patient can only be access by the author until the time the note has been digitally signed. The reason for enforcing this business rule is that unfinished progress note can contain unconfirmed information that should not be used as the basis of action by other clinicians. Clinicians would normally have all the permissions required to read a progress note, so a business rule is implemented to enforce this policy. The application makes use of metadata attributes indicating who the document author is and whether the author has digitally signed to enforce the business rule.

Begin the use case by logging into the application as Dr. Alice (cf. Figure 6).

This section was demonstrated at the RSA 2008 Conference.

2.1.4 Emergency Access

The purpose of this use case is to demonstrate that XACML can be used to enforce emergency overrides of enterprise access control policy. When patient's life or safety is at serious risk, an emergency override of access control policy is a critical requirement. Typically, permissions granted to an actor or role are based on the actor's expected workflow through a process called Role Based Engineering. [HL7 Role Eng] Emergency overrides change the permissions of the actor from this nominal range of permissions to an extended set of permissions providing a greater freedom to access data and functionality. During this period the systems must increase logging activity to capture all access control decisions for future analysis to ensure proper use of the emergency override.

Begin the use case by logging into the application as Dr. Charlie (cf. Figure 1). Dr. Charlie has been assigned to Facility B, and is therefore not allowed to access patient information through the application. In the use case a patient from Facility A presents at a clinic at Facility B suffering from symptoms that require immediate consultation of their medical record. Search on the patient and attempt to access the medical record. Participants may want to out to the booth guests that Dr. Charlie is from Facility B, as shown in Figure 10 below. Note that a medical application would not have allowed Dr. Charlie to get the list of patients in the figure but it simplifies the application.

MPI	name	gender	Date of Birth	Address
160379	SMITH,ANNA	F	Mon May 07 12:05:01 PST 1934	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
462474	SMITH,ANNA	F	Tue Mar 17 12:05:01 PST 1970	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
545591	SMITH,ANNA	F	Tue Feb 23 12:05:01 PST 1999	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
400964	SMITH,HAROLD	M	Wed Dec 13 12:05:01 PST 1961	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
362122	SMITH,JERRY	M	Sun Dec 10 12:05:01 PST 1995	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345
3157	SMITH,LARRY	M	Fri Aug 09 12:05:01 PST 1929	123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345

Figure 10: Dr. Charlie from Facility B selects a patient

Since Dr. Charlie does not have the physician role at facility A, he does not have the permissions required to perform the patient search after selecting the patient name. When Dr. Charlie attempts to search on a patient, the request is denied and the requester is directed to a screen that can be used to declare emergency access as shown in Figure 11.

The PEP - Policy Enforcement Point has determined you do not have permission to access the following resource.

demographics

You may chose to declare an Emergency situation to access the patients record. Do so by clicking on the below "Emergency Override" button. This requires previous granting of necessary priveleges to do so.

Emergency Override

Figure 11: Dr. Charlie attempt at patient search is denied with opportunity to declare an emergency

Dr. Charlie must have the emergency access permission in order to override the access control decision from the PEP. Select the "Emergency Override" and return to the patient search. Dr. Charlie should now

be able to use the application successfully in emergency access mode. Note the application will display the emergency access declaration shown in Figure 12.

The screenshot shows a web application interface with a header bar. The header bar contains the text "Advancing open standards for the information society" and "PDP Provided By: IBM". Below the header bar, there is a form with the following fields: "Name" (SMITH, BAMBI), "Gender" (Male, Female), "DoB" (1952-06-25T00:00:00-07:00), "Facility" (Facility A), and "Emergency Access Declared" (highlighted with a red circle). The "Emergency Access Declared" field is a red button with white text. Below the form, there is a "Chart Cover Sheet" button.

Figure 12: Emergency access banner

The emergency access permission will be passed throughout this operation on the selected patient. If the patient changes, the emergency access declaration must be renewed. At this point participants may want to display the PDP interaction to demonstrate that the PEA-001 is now being passed in the access control request.

2.1.5 Fine Grain Access Control (Data Filtering)

The purpose of this use case is to demonstrate that XACML can be used to express and enforce patient consent directives over parts of the patient medical record displayed to certain providers. This demonstration also shows guests that XACML is efficient enough to determine if parts of the medical record can be displayed as the screen is being displayed. The published use case uses the radiology record in the medical record to demonstrate this functionality.

Participants may start the demonstration by logging into the application as Dr. Bob and displaying the entire medical record. Alternately, the participants can agree with the guest the entire record was displayed previously. If you select the same patient as in §2.1.2 to demonstrate patient consent directives, remember to remove the UBA previously elected by that patient against Dr. Bob.

To add a fine grain constraint directive on behalf of the patient, log into the application as the security administrator (cf. Figure 5) or use the security administrator session you may already have up in a separate browser instance. Search on and select the patient electing the consent directive. As discussed above, the security administrator possesses the SEC-001 privilege, therefore can set consent directives on behalf of the patient. To demonstrate fine grain control that can mask parts of a medical record, use the "Masked Access" link under "Patient Elections" beneath the "Interop Tools" on the left navigation bar, Select the proper Dr. Bob as shown in Figure 13. Use the initial appropriate to the participant.

The screenshot shows a web application interface with a header bar. The header bar contains the text "Advancing open standards for the information society" and "Security, Bob". Below the header bar, there is a form with the following fields: "Name" (SMITH, BAMBI), "Gender" (Male, Female), "DoB" (1952-06-25T00:00:00-07:00), "Facility" (Facility A), and "Emergency Access Declared" (highlighted with a red circle). The "Emergency Access Declared" field is a red button with white text. Below the form, there is a "Chart Cover Sheet" button.

Figure 13: Select the provider that will be disallowed access for the selected patient

After selecting the provider that will be disallowed access for the selected patient, choose radiology as the section of the medical record that will be filtered from the display, as shown in Figure 14.

The screenshot shows a web interface for managing patient records. At the top, there is a form for patient information: Name (SMITH,BAMBI), Facility (Facility A), Gender (Male/Female), and DoB (1952-06-25T00:00:00-07:00). Below this is a section titled "Current Providers with Access Masked By Patient Consent Directive - MA". It contains a table with columns "providerID", "providerName", and "functionalArea". The table is empty, with the text "No results found" and a prompt "Click on 'providerID' to select." Below the table, there is a "Provider name:" dropdown menu showing "Doctor, Bob B". To its right is a "Mask Record Type:" dropdown menu with a list of options: "medical-record", "demographics", "medical-record", "problemist", "procedures", "laboratory", "radiology", "medications", "vitals", and "progress-notes". The "radiology" option is highlighted. To the right of the dropdowns is an "Access Code:" field. Below these elements are three buttons: "Add Constraint", "Remove Constraint", and a partially visible "Reset" button.

Figure 14: Select the part of the record that will be filtered from the provider

Check that the shaded text areas are now properly populated. Select the “Add Constraint” button. The constraint will now appear on the list of current masked access directives for the patient. Note that the access code used to set the constraint is ACRAD, consistent with the HL7 patient constraint vocabulary model.

For this demonstration, the security administrator has added the election made by the patient. This simplifies the demonstration application. Typically, a portal would be used to allow the patient to directly control access to parts of their medical records.

Return to the medical record screen using the proper provider username and demonstrate the effect of removing the permissions. After finishing the demonstration, remember to remove the constraints before reusing the patient in the next demonstration.