Universal Documents System (UDS)

November 5, 2011

Project Summary

There are many agencies that have accumulated vast quantities of hard copy documents over the years of operation. These documents are taking up valuable space which in turn is costing the state of Ohio millions of dollars. The main purpose of this project is to offer a framework for establishing an electronic repository for documents converting our agencies in a paperless environment. Universal Document System was created within the Bureau of Workers’ Compensation and they have offered to collaborate with agencies to establish a UDS system in any agency.

Project Goal

This Project will give State Agencies the framework for a Universal Document System. With this system, we can build a paperless environment. Allow for efficiencies in processing workflow, money saved with the departments, and time efficiencies.

Project Outcome

* Gather Requirements for the use of a Universal Documents System
* Technical Design
* Cost Analysis Plan
* Risk Plan
Project Benefits

The main benefit of the universal document system is that all documents are stored in a single repository. This will eliminating the need for hard copy documents stored and consuming valuable real estate which can be used for more beneficial and efficient purposes.

Project Team

For more information about this project, contact team members

- Hari Gosangi — hari.gosangi@mh.ohio.gov
- Lillian Bouldware – lillian.bouldware@odh.ohio.gov
- Verda McCoy - verda.mccoy@etech.ohio.gov
- Ava Johnson – ava.johnson@odh.ohio.gov
- Jessica McGonigle – jessica.mcgonigle@dodd.ohio.gov
- Mentor – Coach: Nelson Gonzalez
Ohio Department of Developmental Disabilities

UDS Fileroom Admins Guide

Administering the UDS fileroom

11/03/2010
Table of Contents
Overview .............................................................................................................. 3
Managing Users ............................................................................................... 4
Adding Users ................................................................................................... 4
Modify User Information ............................................................................... 6
Security ........................................................................................................... 7
Email ................................................................................................................ 7
Disable/Enable ............................................................................................... 7
Deleting ............................................................................................................. 7
View Change History ...................................................................................... 7
Managing Document Types .......................................................................... 9
Adding ............................................................................................................. 9
Modifying ....................................................................................................... 10
Description ..................................................................................................... 11
Security ............................................................................................................ 11
Archive ............................................................................................................. 11
Active (Disable/Enable) .................................................................................. 11
Deleting ........................................................................................................... 11
View History .................................................................................................... 12
Custom Dropdown .......................................................................................... 14
Adding ............................................................................................................. 14
Enable/Disable ............................................................................................... 15
Deleting ........................................................................................................... 15
View History .................................................................................................... 16
Security Levels ............................................................................................... 18
Users ............................................................................................................... 18
View ............................................................................................................... 18
Update .......................................................................................................... 18
Delete ............................................................................................................. 18
Add ................................................................................................................ 19
Scan ................................................................................................................ 19
Upload .......................................................................................................... 19
Admin .............................................................................................................. 19
Document Type ............................................................................................. 19
Documents ...................................................................................................... 19
FAQ .................................................................................................................. 21
What are common cases of elevation? ........................................................ 21
Overview

The main responsibility of the fileroom administrator is to support the fileroom users. It is expected that fileroom administrators have read and understand the “UDS Fileroom Users Guide” and can reference it to aide fileroom users.

Additional responsibilities include managing user profiles, managing document types (and custom indexes), and managing security through permissions.

Any action that needs to be taken by that is not within the fileroom administrator capabilities should be elevated to the UDS Administrators through the ticket system. For a list of common examples see the FAQ on common cases requiring elevation.
Managing Users

Managing users for the fileroom is done through the Users page. To get to the Users page click the “Users link from the main fileroom.

This brings up the Users page.

<table>
<thead>
<tr>
<th>User ID</th>
<th>View</th>
<th>Update</th>
<th>Delete</th>
<th>Add</th>
<th>Scan</th>
<th>Upload</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHAWN.HOLZWORTH</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TEST.USER</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Adding Users

To add a user to the fileroom, first go to the Users page.

Next click the Add New User button to bring up the Add New Users page.
New users are added to the users list. Each new user should be added to its own line in the new users list. These users can be verified by clicking the “Verify users” button. The user names entered here should be the same ones used by the users to log into windows (i.e. their Windows Login Ids).

Next set the user permissions for the new users.

Now click the “Add User(s)” button to add the users to the fileroom. A confirmation box will appear to confirm you are sure. Click OK to continue.
Next a message box will confirm the users were successfully added, click OK to continue.

The users are now in the fileroom.

Now the users’ accounts can be edited and any other modifications (such as adding email address) can be made.

**Modify User Information**

From the Users page the information for each user id is displayed. The user permissions and email address can be changed as well as whether or not the user is active.

To change this information, click the Edit User button next to the User Id of the user to be edited.
Edit User Button

**UDS - DEVTEST2 Users**

When finished editing the user information, click “Update” to submit the changes.

**Security**
User’s security permissions can be updated from the Users page by editing the user. For more information on the different types of permission see the Security Levels section.

**Email**
When a user is added the email for that account is listed as blank and should be filled in. The email address for each account is used when a user checks out a document. When a user has a document checked out, the user’s email address listed on the User page gives other users a point of contact for the checked out document.

**Disable/Enable**
This switch allows the fileroom administrator to completely disable access to the fileroom for a user (or enable access if it was previously disabled). This provides a solution for accounts that should no longer have access to the fileroom but may need it again in the future.

IMPORTANT: as the site administrator do not disable access to your own account.

**Deleting**
For accounts that are no longer needed the fileroom administrator is able to completely remove the account. If the account may need access again in the future the account should be disabled instead of deleted.

VERY IMPORTANT: as the site administrator do not delete your own account.

**View Change History**

On the User page the fileroom administrator has access to a log containing the history of changes to user accounts. Whenever a user account is added, updated, disabled, enabled, or deleted the changes are logged for future reference.
To access the change history, click the View History link at the top of the User page.

A popup will ask whether to Open or Save the log.

The contents of the file list the date, time, user, repository and action for each of the changes to user information.
Managing Document Types
Each document uploaded into the fileroom is assigned a document type based on the content of the file. Primarily the fileroom administrator will only need to add new document types to the fileroom as needed. However, the fileroom may need to update existing document types, disable document types, or delete them.

Managing document types is done through the Document Types page. To open this page, first go to the main fileroom.

Next click the Document Types link.

**UDS - DEVTEST2**

| UDS Help | Reports | Users | Document Types | M |

This will bring up the Document Types page.

**UDS - DEVTEST2 Document Types**

Here the fileroom administrator is able to add new document types, edit existing document types, delete document types, and view the update log for document types.

**Adding**
To add a new document type to the fileroom, the fileroom administrator first needs to open the Document Types page.

Next, click the Add New Document button to bring up the Add New Document Type page.

Add New Document Button
Next the fileroom administrator must fill out the information for the document type being added.

Document Type: The 9 character short name for the document type
Document Description: The 50 character description of the document type
Security level: The 0-100 minimum security level for the document (see Security Levels)
Archive Status: Whether or not documents of this type are archived
Document Retention: How long documents of this type are retained

When finished click the Add New Document Type button.

Modifying
To begin editing the information for an existing document type, first open the Document Type page.

Next click the Edit Document Type button next to the document type to be edited.
Edit Document Type Button

This makes the document type editable. On this page the fileroom administrator is able to edit the description, security level, archive status, and retention date. The fileroom administrator can also enable or disable a document type.

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Description</th>
<th>Security Level</th>
<th>Archive Status</th>
<th>Days To Archive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARCHIVE</td>
<td>ARCHIVE DOCUMENT</td>
<td>50</td>
<td>1</td>
<td>365</td>
<td>Yes</td>
</tr>
<tr>
<td>CONF</td>
<td>CONFIDENTIAL</td>
<td>90</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>PCB</td>
<td>PUBLIC DOCUMENT</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>TEST</td>
<td>TEST DOCUMENT</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
</tbody>
</table>

When done editing the document type, select the Update link to commit the changes.

Note: when fields for a document type are change, this applies only to future documents of this type. Existing documents need to be edited individually.

**Description**

The description describes the document type in at most 50 characters. This is the default description used for new documents assigned this document type. When adding documents a user can modify the description to better describe the document if they wish.

**Security**

The security level of the document, see [Security Levels](#) for more information.

**Archive**

The archive status is whether or not archiving is used for the document. If archiving is active, when a document of this type is added its archival date (date of archiving) is set to the date the document was added plus the number of days in the Days to Archive field.

**Active (Disable/Enable)**

When a document type is active and a user adds a document that document type is available in the drop down list for document types. A disabled document type is not available to the user when adding documents but can still be selected when searching.

**Deleting**

Deleting a document type completely removes it from all document type lists (adding, searching, updating, document type page). A document type can only be deleted if a document of this type has not been indexed yet. If a document has already been indexed of this type it should be deactivated instead of deleted.
To delete a document type, go to the document type page.

Click the Delete Document Type Button.

Delete Document Type Button

Click OK to delete the document type. The document type is now deleted. However, if the following pop up box appears the document type already been used and cannot be deleted. To prevent further documents from using this type it should be disabled instead.

View History

To view the update history for document types, first go to the document type page.

Click the View History link.
Next the file download dialog will prompt you to Open or Save the log.

The contents of the file list the date, time, user, repository and action for each of the changes to document type information.
**Custom Dropdown**

In the fileroom some custom search fields are displayed as drop down lists. Fileroom administrators are able to add new options to these dropdown lists, enable/disable the existing options, and delete options. Fileroom administrators can also view the update history for dropdown options.

Managing dropdown options is done through the Dropdown Option page. To open this page, first go to the main fileroom.

Next click the link for the drop down option (in this example, “Mark”).

![Dropdown Option Page](page.png)

This will bring up the page for that dropdown.

Here the fileroom administrator is able to add new options, enable/disable existing options, delete options, and view the update log for the options.

**Adding**

To add a new option to the fileroom, the fileroom administrator first needs to open the page for that dropdown.

Enter the name of the dropdown option in the textbox and click Add to add the option.

When the option is successfully added a confirmation box will appear.
Click OK, the options has been added to the drop down list.

**Enable/Disable**

The options in a dropdown list can be enabled or disabled from the administrator page for the dropdown. To enable or disable an option first go to the administrator page for the drop down.

Next click the Edit Option button next the option to edit.

Now the fileroom administrator can change whether an option is active or not. Inactive options do not show in the dropdowns for adding documents (they still show up when searching).

**Deleting**

Deleting a dropdown option completely removes it from all dropdowns (adding, searching, updating, dropdown administrator page). An option can only be deleted if a document of this type has not been indexed yet. If a document has already been indexed using that dropdown option the option should be deactivated instead of deleted.

To delete an option, go to the administrator page for the dropdown.

Click the Delete Option Button.
Click OK to delete the option. The option has now been removed from the dropdown. However, if the following pop up box appears the option has already been used and cannot be deleted. To prevent further documents from using this option it should be disabled instead.

View History
To view the update history of the dropdown, first go to the admin page for the dropdown.

Click the View History link.

Next the file download dialog will prompt you to Open or Save the log.
The contents of the file list the date, time, user, repository and action for each of the changes to the dropdowns.
Security Levels

Security levels provide the main means of limiting access to documents. The fileroom administrator can control the security levels of individual users, documents, and document types.

Security levels are specific only for each fileroom. This means each user can have different security levels for different filerooms. An example of this would be a user having administrative rights to one fileroom and only view access to another.

Users

User security in the fileroom is a top down approach. What this means is that if an action for a user (such as View) is set at level 50, then that user can view all documents whose security level is 50 or lower.

See also:
Changing User Security Level

View

View permissions control what documents are visible to the user during searches. This permission is in the range of 0 to 100 with 100 being highest security (a person with 100 view level can see all documents). This also includes whether or not a user is able to download the document. If a user is given the download link for a document with a higher security level than they can see, the download dialog will not appear when they click on the link.

Update

View permissions control what documents a person can checkout or update. This permission is in the range of 0 to 100 with 100 being highest security (a person with 100 update level can check out all documents).

Delete

Delete permissions control what documents a person is able to delete (barring other restrictions). This permission is in the range of 0 to 100 with 100 being highest security (a person with 100 delete level can delete all documents). It is recommended that this security permission be restricted to only a small number of users (possibly admin only depending on your department’s retention policy)
**Add**
The add permission level determines whether or not a user is able to upload, scan, or otherwise insert documents into the fileroom system. If a user can add documents the value is 1, otherwise the user cannot add any documents.

**Scan**
The scan permission determines whether or not a user is able to scan documents into the fileroom using a scanner and the Kodak Capture Pro Software. A value of “Yes” gives the user this capability. This permission should be combined with a 1 in Add permissions for users of the scanning software.

**Upload**
The upload permissions determine whether or not a user is able to use the upload page to insert documents directly into the fileroom. A value of “Yes” gives the user this ability. This permission should be combined with a 1 in Add permissions for users who will be adding documents through the upload page.

**Admin**
The admin permission gives the user admin capabilities. An admin user is able to change security levels for users, documents, and document types. Admin users can also add/modify/delete users, document types, and dropdown options. These capabilities are in addition to the users other permissions; they do not supersede the other rights, for instance, an administrator who does not have delete permissions is not able to delete documents.

WARNING: Do not remove your own admin rights, especially if you are the sole admin for your fileroom. You will need to put in a ticket to get them back.

**Document Type**
The security level for a document type is a single number from 0 to 100. This number is used as the default security level for any document created with this document type.

See also:
[Changing Document Type Security Level](#)

**Documents**
The security level for a document is a single number from 0 to 100. This number is used in combination with the user’s security permissions to determine what actions that user can take with this document.

The default value for this number is determined by the document type the document was created under. The security level can be changed for individual documents by editing the documents as a fileroom administrator.

**Security Examples**
Here are some examples to show how the fileroom security works.
Using these settings USER.ONE can upload but not scan documents; USER.TWO can scan but not upload through the fileroom; USER.THREE cannot add any documents; and user four can scan and upload.

Example one: Document with security level 50. This document can be viewed by all users except USER.THREE, can be updated by USER.TWO and USER.FOUR, and can be deleted by none of these users.

Example two: Document with security level 90. This document can be viewed by USER.ONE only and cannot be updated or deleted by any user.

Example three: Document with security level 50. This document can be viewed by all users except USER.THREE, can be updated by USER.TWO and USER.FOUR, and can be deleted by none of these users.
FAQ

What are common cases of elevation?

These are a few common causes that would require elevating an issue from the fileroom admin level to the UDS admin level.

- A document that was deleted needs to be restored.
- The only administrator has deleted, deactivated, or removed permissions from their account.
- A user has checked out a document, and gone on vacation.
- A modification to the site has been suggested.
Business Case:

State Agencies will have the knowledge and framework for a Universal Document Service (UDS). With this system, a paperless file room can be built to store documents and files. Allow for efficiencies in processing workflow, money saved within the department, and add time efficiencies.

Overview/History of Product:

The UDS system was custom built for the Bureau of Workers Compensation (BWC). UDS contained multiple department sites, core fields, specific fields, and minor customizations. As of today, along with BWC, there are two other State agencies that have implemented UDS as there file storage, Ohio Shared Services and the Department of Developmental Disabilities (DODD).

Benefits:

UDS is a “home grown system” and remains the agencies “one of a kind”
UDS is generic and can be easily customized
UDS can be compatible to most infrastructures and servers
UDS can for most agencies be implemented in 6-8 months

Negative:

UDS is dependent on agency requirements
State Agency has to maintain technical support for UDS
Security: e.g. Windows authentication

Database/Servers:

SQL
IIS
Fileserver
SANS
.NET
Oracle

Additional Equipment:

Scanners-if agencies have back filing that will need scanned
Licenses for any additional servers
Any additional programs for integration pieces
Cost:

UDS can be a low cost implementation for most agencies if the agency already contains the needed databases and servers. DODD’s cost for the six-month project was +/- $105,000.00. DODD only needed to purchase scanners, an email integration piece called “Black Ice”, and the cost for the Subject Matter Experts (SME). DODD already had all the necessary databases and servers.

Pre/Post Preparation:

Chief Information Officers (CIO) will need to get the source code from DODD or BWC Consultants for UDS will then need to be contacted for requirements gathering Department Tech support for when SME contracts are up

Department Tech Support:

Consultants do not support the Application/Server Consultants will start and finish implementation then transition to the agency

Agencies should have someone to take over the tech support once the consultant’s contract is up. An ideal candidate should have some of the following education:

- Developer experience
- Programming
- Analysis
- Customer service
- SQL experience
- IIS experience
- Web service
- .NET experience
- Database experience
Indexing—How do you file documents today?
Choose one or more of the following:
- Policy #
- Claim #
- DODD #
- Employee #
- Medicaid #
- Project #
- Provider #

List additional fields you file by (not including document type and date received). If none apply above please make your list below.

Please indicate the fewest fields needed to run your business area. Additional indices mean more work for your users.

Throughput—How many documents do you work with?

Paper—how many pages are stored in your area IN ONE YEAR
- Under 10
- 10-100
- 100-1000
- 1000-10000
- 10000-100000
- Over 100000

Incoming Fax—how many pages arrive in your area IN ONE YEAR
- Under 10
- 10-100
- 100-1000
- 1000-10000
- 10000-100000
- Over 100000

Electronic documents—how many documents are stored in your area IN ONE YEAR
- Under 10
- 10-100
- 100-1000
- 1000-10000
- 10000-100000
- Over 100000

Does your area store audio or video files?  Yes  No

Document Types—What kinds of content do you work with?

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Document Description</th>
<th>Document Retention</th>
<th>Special Security?</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 characters max</td>
<td>30 characters max</td>
<td>If based on Policy, please provide</td>
<td></td>
</tr>
</tbody>
</table>
### Document Types continued

<table>
<thead>
<tr>
<th>Document Type 10 characters max</th>
<th>Document Description 30 characters max</th>
<th>Document Retention If based on Policy, please provide</th>
<th>Special Security?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
</tbody>
</table>

### Users—Who in your area will be using UDS?

<table>
<thead>
<tr>
<th>Team or Role</th>
<th>Last Name</th>
<th>First Name</th>
<th>User Name (A#)</th>
<th>PC #</th>
<th>View</th>
<th>Update</th>
<th>Delete</th>
<th>Scan</th>
<th>Upload</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
### Users continued

<table>
<thead>
<tr>
<th>Team or Role</th>
<th>Last Name</th>
<th>First Name</th>
<th>User (A#)</th>
<th>PC #</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes**—Please enter any explanations or details here
Directions

Indexing

- Review your current method for filing documents, both paper and electronic
- Are there additional fields/codes/folders/subfolders/indices you do or could use? Please list a maximum of two of these in the space provided.
- If you file by content, these can be included as document types (see below) rather than separate indices
- Please keep in mind the following:
  - Both the document type and the date the document is received will already be included as document indices, so they should not be listed as additional fields here
  - Indices should be kept to the minimum required to run your business area
  - Additional indices above that will only mean more work for your users when adding documents

Throughput

- For the area you are representing, how many pages/documents will need to be stored annually?
- For paper and incoming faxes, this should be listed by number of pages
- For electronic documents (any onscreen document that can be changed by the user), this should be listed by the number of documents, not the number of pages
- Certain areas store audio and/or video electronic files—please indicate if this is so, and the project team will work with you to get details

Document Types

- Document Types are based on the content, not the format, of the document
- Review all documents used in your area, and build a list of document types based on this.
- The Document Type name used can be no longer than 10 characters, and is usually an abbreviation of the Document Description, which can be no longer than 30 characters. Some examples:
  - FMLA
  - Employee information
- UDS ties retention to document type, and keeps track of this for a deletion process
- Most document types will be available to your area in general, but some should be limited to specific personnel or made available outside of your area to others. If this is the case, please indicate if this is so under “Special Security”, and the project team will work with you to get the details.

Users

- Build or locate a list of users in your area
- The team or role will be based on the tasks of the user, or if they work in a particular unit
- User Name refers to their main login, normally listed as a number starting with “A”
- PC # is the code listed on the barcode sticker. It is also normally listed on the user’s desktop as “My Computer X999999”.
- The six boxes to the right of each user indicate the rights that user should have.
  - View—most if not all users will have access to view documents
  - Update—the users you indicate will also be able to update a document
  - Delete—deletion of documents is generally not allowed—your area will make the call on who, if anyone, is allowed to do so
  - Scan—depending on the setup of your paper processes, certain personnel will be allowed to scan documents
  - Upload—in addition, you may wish to allow specific users to upload documents from their desktop
  - Admin—one or two users from your area will act in an Admin capacity, with additional functionality and responsibility

A Notes area is provided if you have any other details or explanations.

Please contact your assigned liaison if you have any questions or concerns.
Customer Worksheet

<table>
<thead>
<tr>
<th>Department</th>
<th>Dept Name:</th>
<th>Dept Fax No:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Main Contact Name:</td>
<td>Phone No:</td>
</tr>
<tr>
<td>Number of users in department:</td>
<td>Expected per-user document access: once every 1 Month(s)</td>
<td></td>
</tr>
<tr>
<td>Expected throughput: pages every Month</td>
<td>Describe Indexing Elements (Are there numbers or codes used in your dept? Are documents stored by date? Is a description or abstract created?):</td>
<td></td>
</tr>
</tbody>
</table>

Describe your overall departmental workflow:

Describe any record retention schedules for your department established by policy and/or Ohio Revised Code:

Describe any requirements for redaction of documents and or content for your department established by policy and/or Ohio Revised Code:

Enter Names of all users in your department (or provide list separately):
**Customer Worksheet**

*Note: Estimates of quantities on this page are acceptable.*

**Scanning - Enter Expected Quantities for each category**

<table>
<thead>
<tr>
<th>Scan quantity:</th>
<th>pages per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of double-sided pages:</td>
<td>0%</td>
</tr>
<tr>
<td>Percentage of non letter-sized pages:</td>
<td>0%</td>
</tr>
<tr>
<td>Percentage of documents with colored text or graphics:</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Faxing - Enter Expected Quantity**

<table>
<thead>
<tr>
<th>Inbound: faxed pages per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound: faxed pages per Month</td>
</tr>
</tbody>
</table>

**Electronic Input - Non-image documents**

<table>
<thead>
<tr>
<th>Expected quantity: pages per Month</th>
</tr>
</thead>
</table>

**Document Types - Enter appropriate information for ALL document types**

<table>
<thead>
<tr>
<th>Document Type Name</th>
<th>Ability to Edit Document?</th>
<th>Workflow Specific?</th>
<th>Record Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☐ Yes ☐ No</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Please provide hard-copy samples of each document type.*

**Backfile**

- Expected backfile pages (paper or electronic):
- Expected timeframe to complete:
- Expected staffing to perform backfile (prep, scan, index):
- Is there a mandate (legal, admin) to perform backfile?: ☐ Yes ☐ No

What are the benefits of performing the backfile?:

Current Disaster Recovery Plan requirements and possible benefits of backfile:
Universal Document Storage System

Paperless Matrix
Project Objectives
Overview

Universal Document Storage System

Streamline

Secure

Efficient

Paperless
Business Case

File Systems
- Mismanagement
- Space requirements
- Process time

Paperless Environment
- Easy retrieval
- Efficient work environment
- Audit trail and accessibility
Objectives

1. Requirements to create UDS
2. Meet with SME
3. Gather requirements
4. Create Project Work Breakdown Structure (WBS)
5. Create Product Booklet
6. Create Product WBS
7. Conduct Presentation
In/Out of Scope
In Scope

- Gather Requirements
  - Subject Matter Expert (SME)
- Human Resources
- Technical Staff
Out of Scope

- Business Requirements
- Vendor Selection
- Approval of Product
Project Work Break Down
Schedule and Cost
Project Hours

Planned Work versus Actual Work Progress Report

Project Time-line by Week

Planned Work
Actual Work
## Project Cost

### Project Progress Dashboard - Paperless Matrix Team

<table>
<thead>
<tr>
<th>WK1</th>
<th>WK2</th>
<th>WK3</th>
<th>WK4</th>
<th>WK5</th>
<th>WK6</th>
<th>WK7</th>
<th>Project’s Total Estimated Work</th>
<th>Project’s Total Actual Work</th>
<th>Blended Rate ($0.00/hr.)</th>
<th>BAC</th>
<th>MS Office Project Total Work</th>
<th>Project Work Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$50.00</td>
<td>$11,050.00</td>
<td>$13,800.00</td>
<td></td>
</tr>
</tbody>
</table>

| Estimated Planned Work | 32.5 | 32.5 | 32.5 | 26.0 | 32.5 | 32.5 | 32.5 | 221.0 |                       |                       |               |
| Planned % Complete     | 14.7% | 14.7% | 14.7% | 11.8% | 14.7% | 14.7% | 14.7% |               |                       |                       |               |
| PV                      | $1,625.00 | $1,625.00 | $1,625.00 | $1,300.00 | $1,625.00 | $1,625.00 | $1,625.00 |               |                       |                       |               |

| Actual Work Complete   | 32.5 | 37.5 | 44.0 | 36.5 | 44.5 | 43.5 | 37.5 | 276.0 |                       |                       |               |
| Actual % Complete      | 14.7% | 17.0% | 19.9% | 16.5% | 20.1% | 19.7% | 17.0% |               |                       |                       |               |
| EV                      | $1,625.00 | $1,875.00 | $2,200.00 | $1,825.00 | $2,225.00 | $2,175.00 | $1,875.00 |               |                       |                       |               |
| SPI                     | 1.00 | 1.08 | 1.17 | 1.22 | 1.25 | 1.27 | 1.25 | $2,750.00 |               |                       |               |
Risk Plan
Risk Management Process

**IDENTIFY**
possible risks and threats to project

**IDENTIFY**
potential impact on project

**DETERMINE**
how to classify and prioritize risks

**DETERMINE**
most effective way to resolve risks
SWOT Analysis

**Strengths**
- Team members are multi-talented, i.e., mixture of MBTIs
- Several team members are experienced in project’s subject matter
- Team members are committed to the project

**Weaknesses**
- Unforeseen schedule conflicts
- SMEs may not be available at a specific time
- SharePoint may not be accessible for uploading documents

**Opportunities**
- Project team members are made aware of project’s benefits
- Project Team member’s respective agencies will be able to replicate project with ease
- Subject Matter Experts are available to team

**Threats**
- Quality of project could be compromised due to lack of time to complete deliverables
- Team members will not be able to contribute their fair share
- Technical difficulties
### Risk Analysis Log

**Risk Legend:** 1 is low risk, 5 is high risk

<table>
<thead>
<tr>
<th>Date Identified</th>
<th>Risk Category</th>
<th>Potential Impact</th>
<th>Risk Owner</th>
<th>Probability of Occurrence</th>
<th>Impact of Probability</th>
<th>Level of Risk</th>
<th>Contingency Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/6/11</td>
<td>HR</td>
<td>Delay in completing project on time due to team schedule conflicts</td>
<td>Team</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>Review scope, schedule and reassign work if necessary</td>
</tr>
<tr>
<td>10/6/11</td>
<td>IT</td>
<td>Technical Difficulties</td>
<td>Team</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>Identify other ways to communicate with team members</td>
</tr>
<tr>
<td>10/6/11</td>
<td>Resources</td>
<td>SME may not be available when needed</td>
<td>Team</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>Identify more than one SME</td>
</tr>
</tbody>
</table>
Assumptions and Constraints
Assumptions

SME Availability → Framework For Product Implementation → Knowledge to Enhance Skills
Constraints

- Technical Difficulties
- Six Weeks
- Schedule Conflicts
Communications Plan
# Communications Plan

<table>
<thead>
<tr>
<th>Event</th>
<th>Target Audience</th>
<th>Message objective</th>
<th>Timing</th>
<th>Vehicles</th>
<th>Sender</th>
<th>Feedback Mechanism</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Core Team Communication</td>
<td>Team</td>
<td>Communicate plans, decisions and agreements re: project and product</td>
<td>Daily</td>
<td>E-mail, face-to-face, SharePoint, Conference Calls</td>
<td>Team</td>
<td>E-mail, face-to-face, SharePoint, Conference Calls</td>
<td>Review the project - Decision Making</td>
</tr>
<tr>
<td>Weekly Project Status Updates</td>
<td>Team, PMP Instructor</td>
<td>Project Status updates</td>
<td>Every Thursday</td>
<td>E-mail, SharePoint, Conference call</td>
<td>Team</td>
<td>Email, SharePoint</td>
<td>Decisions and Project/Product Progress</td>
</tr>
<tr>
<td>Meeting Agenda</td>
<td>Team</td>
<td>Communicate action items, project schedule, outstanding items</td>
<td>Every Thursday</td>
<td>Face-to-Face</td>
<td>Project Manager</td>
<td>Email, SharePoint, Face-to-Face</td>
<td>Review Project/Product Progress</td>
</tr>
<tr>
<td>High Level Project Status Updates</td>
<td>Team, PMP Instructor, SME</td>
<td>Communicate action items, review product status</td>
<td>10/13/2011</td>
<td>Face-to-Face</td>
<td>Project Manager</td>
<td>Face-to-Face</td>
<td>High Project guidance</td>
</tr>
<tr>
<td>Presentation</td>
<td>Directors, Managers, Supervisors, Other Guest &amp; Cohort Members</td>
<td>Deliver presentation</td>
<td>11/3/2011</td>
<td>PowerPoint</td>
<td>Team</td>
<td>Face-to-Face</td>
<td></td>
</tr>
</tbody>
</table>
Quality Control
QUALITY CHECKLIST

- Project presentation template will be created and used by all team members.
- Is formatting standard and consistent?
  - Is grammar and spelling correct?
- Are approved changes integrated with end product?
- Project documents will be posted to SharePoint and reviewed before class. All team members are responsible for reviewing project documentation.
  - Assigned team roles (editor, scribe, document management) and agree to Code of Conduct.
- Use the SharePoint site provided for the class.
  - Presentation walkthrough on 10/27/2011.
Lessons Learned
Lessons Learned

What Worked

- Continuous design, code reviews, referring to functional specs.
- Having right resources and SME's on the team.
- Regular team and technical meetings.
- Entire team committed to project schedule.

What Didn't Work

- Use of SharePoint as main communication tool.
- Working on project in silos.
- Unexpectedly had to re-do some work.
- Budget constraints.

Any Surprises

- Schedule conflicts.
- MBTI cohesiveness.
- SharePoint access issues.

What will we take away

- Address any issues early in the project.
- It is better to work as a team.
Product Overview
Work Break Down

Paperless Matrix

- Procurement
  - Networking
  - Softwares
  - Hardware or Servers

- Installations
- Front End Development
- Testing
  - Testing of Network Config of Servers
  - Testing of Actual Front End Code
  - 3 Developers Java/Net
    - DBA
      - Manager
  - Install Developers Tools
  - Task List / Activities
  - Software Installations
  - C5 Installations
  - AUX / LINUX
    - NETWORK Configuration
  - App. Server Installs
  - Database Installs
WBS (Cont.)

- Scan CLOD Documents
- Meetings
- Documentation
- Training Employees
- Support
  - Group Trainings
  - Individual Trainings
  - 24X7 Support/App. Support
    - Help Desk
      - Tickets Assignment
- Cell Phone/Picture Capture
- Scanners
- Fax Machines
  - weekly/monthly
  - Appreciation of Staff
  - Share Point/Online Docs
  - Technical Docs
    - Daily Status/Weekly Status Reports
    - Next Week Tasks
    - Awards/Rewards
    - Goals
DODD UDS Example

Universal Document Repository

Logout

Please click on the UDS repository that you want to use.

UDS - CB CERT
UDS - HEARINGS
UDS - PASRR
UDS - PRIOR AUTHORIZATION
UDS - PROVIDER CERT
UDS - WAIVER
DODD UDS Cont.
<table>
<thead>
<tr>
<th>Document Type</th>
<th>Description</th>
<th>Security Level</th>
<th>Archive Status</th>
<th>Days To Archive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>502</td>
<td>INFORMATION REQUEST &amp; RESULTS</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>APOLOGY</td>
<td>APOLOGY NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>COW</td>
<td>CHANGE OF WAIVER</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>DENL LTR</td>
<td>DENIAL NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>DISE LTR</td>
<td>DISENROLLMENT NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>ENRL LTR</td>
<td>ENROLLMENT NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>HISTORY</td>
<td>HISTORY DOCUMENT</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>INCO LTR</td>
<td>INCOMPLETE APPLICATION NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>INDN LTR</td>
<td>INTENT TO DENY NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>INELIG LTR</td>
<td>INELIGIBLE LETTER</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>INIT APPL</td>
<td>INITIAL WAIVER APPLICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>INIT LTR</td>
<td>INITIAL ENROLLMENT NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>LOC DATE LTR</td>
<td>LEVEL OF CARE DATE CHANGE FORM</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>LOM LTR</td>
<td>LOSS OF MEDICAID NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>MED EVAL</td>
<td>MEDICAL EVALUATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>NICS 1</td>
<td>NOTIFICATION OF INDIVIDUAL CHANGE IN STATUS—PART 1</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>NICS 2</td>
<td>NOTIFICATION OF INDIVIDUAL CHANGE IN STATUS—PART 2</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>OTHER</td>
<td>MISCELLANEOUS DOCUMENT</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>PL DOC</td>
<td>PATIENT LIABILITY SUPPORT DOCUMENT</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>PLOM LTR</td>
<td>POSSIBLE LOSS OF MEDICAID NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>PNO LTR</td>
<td>PRIOR NOTICE OF DISENROLLMENT NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>PSYC EVAL</td>
<td>PSYCHOLOGICAL ASSESSMENTS</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>RDSC APPL</td>
<td>REDETERMINATION SIGNIFICANT CHANGE</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>RDSC LTR</td>
<td>REDETERMINATION SIGNIFICANT CHANGE LETTER</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>REDT APPL</td>
<td>REDETERMINATION OF LEVEL OF CARE ELIGIBILITY</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>REDT LTR</td>
<td>REDETERMINATION NOTIFICATION</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
</tr>
</tbody>
</table>
UDS Document Flow (DODD)
2-tier architecture
Special Thanks

Subject Matter Expert: Dharmesh Patel

Project Manager
Instructor: Nelson Gonzalez

All Team Member’s Managers
Q &A