110 Horizon Drive, Suite 210, Raleigh, NC 27615
919.459.2070

Land Records Management System Best Practices

Adopted by the PRIA Board on December 19, 2018

http://www.pria.us

PROPERTY RECORDS INDUSTRY ASSOCIATION

Copyright Notice, License, Disclaimer

For

PRIA Completed Work Product

March 2019

A. **COPYRIGHT NOTICE**: Copyright © 2019 – Property Records Industry Association ("PRIA"). All rights reserved.

B. **LICENSE:** This completed PRIA work product document (the "Completed Work") is made available by PRIA to members and the general public for review, evaluation and comment only. This document is under development and not a final version.

PRIA grants any user ("Licensee") of the Completed Work a worldwide, royalty-free, non-exclusive license ("License") to reproduce the Completed Work in copies, and to use the Completed Work and all such reproductions solely for purposes of reviewing, evaluating and commenting upon the Completed Work. NO OTHER RIGHTS ARE GRANTED UNDER THIS LICENSE AND ALL OTHER RIGHTS ARE EXPRESSLY RESERVED TO PRIA. Without limiting the generality of the foregoing, PRIA does not grant any right to: (i) prepare proprietary derivative works based upon the Completed Work, (ii) distribute copies of the Incomplete Work to the public by sale or other transfer of ownership, or (iii) display the Completed Work publicly. Comments on the Completed Work must be sent to PRIA.

Any reproduction of the Completed Work shall reproduce verbatim the above copyright notice, the entire text of this License and the entire disclaimer below under the following header:

This document includes Completed Works developed by PRIA and some of its contributors, subject to PRIA License. "PRIA" is a trade name of the "Property Records Industry Association." No reference to PRIA or any of its trademarks by Licensee shall imply endorsement of Licensee's activities and products.

C. **DISCLAIMER: THIS COMPLETED WORK IS PROVIDED "AS IS." PRIA AND THE AUTHORS OF THIS INCOMPLETE WORK MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT; (ii) THAT THE CONTENTS OF SUCH COMPLETED WORK ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; AND, (iii) THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. IN NO EVENT WILL PRIA OR ANY AUTHOR OF THIS COMPLETED WORK BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS COMPLETED WORK, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA ON ANY INFORMATION HANDLING SYSTEM OR OTHERWISE, EVEN IF PRIA OR THE AUTHORS OR ANY STANDARD-SETTING BODY CONTRIBUTORS TO THIS COMPLETED WORK ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

Table of Contents

EXECUTIVE SUMMARY

A Land Records Management System (LRMS) provides a mission critical connection between government and business sectors in the property records industry. These software products provide solutions to many technical, regulatory, and statutory requirements that recording jurisdictions face in the United States. LRMS products are vital for recording jurisdictions to operate efficiently and effectively.

This Property Records Industry Association (PRIA) work product provides recording jurisdictions with information, which may be helpful for evaluating and making informed decisions about LRMS solutions. It also provides a comprehensive set of best practices for the LRMS vendors to consider when developing or implementing products.

Evaluating an LRMS offers the recording jurisdiction the opportunity to review current workflow. In some cases, office processes and procedures have been built around the constraints of a legacy LRMS. New systems have an abundance of features and functionalities, so it is important to evaluate the impact of these technologies. This paper does not address the professional services provided by the vendor that jurisdictions will need to engage to implement and maintain the LRMS.

An effective LRMS should have the ability to adapt to the changing demands and requirements of the recorder's office. The recording jurisdiction should also consider the existing functional capacity of the LRMS and the software vendor's commitment to support, maintenance, and future innovation.

While the LRMS procurement process (e.g., proposal requests, contract procedures or product demonstrations) is not addressed, this paper does provide several areas to consider. Recording jurisdictions range considerably in size, volume, requirements, and funding availability. The intent of this work product was to incorporate a wide range of topics for consideration, realizing not every topic or best practice will apply to every jurisdiction.

Past PRIA work products have addressed property recording processes, including bulk records access, records preservation, indexing, redaction, the Uniform Real Property Electronic Recording Act (URPERA), eNotarization, and eRecording. This LRMS Best Practices document brings together components of previous PRIA work products with a focus on how LRMS solutions support the property records industry.

PREPARATION AND SYSTEM PLANNING

Infrastructure

The infrastructure supporting an LRMS is critical to that system's ability to perform efficiently. Server and network capacity, up-to-date operating systems and databases, provisions for disaster recovery, testing or training environments, and protection against computer viruses, including malware and ransomware, all play a role in the reliability of an LRMS. Additional considerations may apply if the LRMS is hosted by the vendor (referred to as "cloud-based"). Each LRMS vendor will make specific recommendations for the product they provide but this section describes some typical components.

Hardware

Servers are comprised of multiple processors, memory, and available disk space for storage. Servers may be dedicated or virtualized. Consultation between the jurisdiction's IT professionals and the LRMS provider's IT professionals is vital prior to the acquisition of servers to assure the hardware will meet the needs of the LRMS for the present and future years. The number and configuration of those servers may vary depending on the recommended requirements of the specific LRMS, and often include separate servers for the application and the database.

Separate servers or environments for testing or training should be configured to meet the jurisdiction's needs. Additional servers should be acquired for an environment where public access is desired or required. Public access to LRMS records should not be provided through the county's production servers to protect against potential security breaches and to avoid competition for server and resource bandwidth.

As a best practice, the recording jurisdictions should establish separate servers or databases for production, testing or training, and web applications. All servers should reside inside the firewall with limited open ports for external customers.

Server configurations often include multiple processors with multiple cores, sufficient computer memory to execute LRMS program instructions without delay, and disk space that may range from 500 GB to multiple terabytes (TB) for image and index data storage. Sizing for each server's configuration should be based on current volumes, projected growth, desired performance, and any expected back-file conversion projects that may add significant storage requirements. The jurisdiction should consider utilizing stress testing for both the network and system levels.

Industry standard server warranties should be acquired. Due to the frequent improvement in server technology and equipment obsolescence, the regular replacement of servers beyond the extended warranty period should be incorporated into the LRMS planning and budgeting process. Attempting to

extend the lives of servers beyond manufacturer warranty periods poses serious risks for interruptions of service and an inability to obtain parts for any repairs that may be required.

Computer workstations are the employee-facing devices that are also essential to the LRMS. Minimum requirements may vary for workstation types and these minimum requirements should be available from the LRMS vendor. Considerations should include processor, memory and disk space recommendations, operating system recommendations, network communications capacity, and options for multiple monitor support.

Peripheral equipment such as receipt printers, label or bar code printers, cash drawers, check scanners, large format map/plat scanners and printers, and laser printers should not be overlooked. A number of peripherals make use of manufacturer-specific software drivers that govern their operation. Thus, peripheral devices from one system may not be compatible with another LRMS. For example, recording jurisdictions may wish to consider using laser printers in place of specialized receipt printers. More standardization exists for laser printers based on a printer command language (PCL) and for scanners based on current industry standards. A jurisdiction's LRMS vendor should provide specific peripheral recommendations.

Warranties and support for peripheral equipment varies widely and should be considered depending on the specific device involved. Specialized receipt printers and endorsing equipment typically experience relatively heavy use and may be prone to more frequent mechanical breakdown than other devices.

As a best practice, an LRMS system should include server, workstation, and peripheral hardware that are configured to ensure the efficient operation of the application.

Server Virtualization

Server management often is centralized within an IT department. To make the most efficient use of investments in servers, IT departments often rely on virtualized servers so that multiple server environments can reside together on the same physical machine; this approach helps alleviate the need to purchase additional physical servers to manage the variety of applications used by multiple departments. Consultation and collaboration between the recording jurisdiction's IT department and the LRMS vendor's IT team should ensure sufficient server resources would be available for the optimal operation of the LRMS software.

Network

Networks govern the amount and speed of information transferred between servers and workstations and other peripherals within a jurisdiction's offices. Network capacities have increased over time, are most often measured at either 100 megabits per second or 1 GB per second, and may be hard-wired or wireless. The reliability of a jurisdiction's internal network can impact the reliability of operations for an

LRMS and should be considered during the acquisition process. Consideration should be given to peak operating periods over the entire network to ensure efficient data and image transfer speeds.

Operating System and Database Management System Software

The Operating System (OS) and Database Management System (DBMS) are essential components of the LRMS. Operating System software, such as Microsoft Windows and LINUX, are by nature proprietary. Ensuring that the operating system is supported by the OS vendor and that it is updated with patches and new versions over time is important to protect the integrity of the LRMS.

DBMS software should also be currently supported and updated with patches and new versions that also are supported by the LRMS vendor. Jurisdictions should make use of non-proprietary DBMS that are referred to as relational database management systems (RDBMS), such as Microsoft SQL and Oracle. Proprietary databases often make conversions to future systems difficult and costly.

Infrastructure Protection

It requires planning to protect the integrity of the LRMS, its supporting database, operating system and hardware against computer viruses, keylogging, malware, ransomware and unauthorized intrusion. Items to consider include specific software protection; adoption of policies and procedures governing internet access, plus password changes and protection; ongoing system monitoring for intrusion detection; and external internet traffic evaluation. Protection of the infrastructure is a partnership between the LRMS vendor and the jurisdiction. LRMS vendors should be consulted regarding compatible anti-virus, anti-malware, and other application software. Public access to documents and index data should be managed through other servers inside the jurisdiction's software firewall. These protections are accomplished, in part, by the use of reverse proxy servers, which are configured to process a public search, collect the information requested from the jurisdiction's servers, and provide the results without enabling direct public access to the jurisdiction's servers.

As a best practice, an LRMS system should include protection from virus, malware, key logging, ransomware and other externally introduced threats. Additional steps should be taken to protect the infrastructure in the event of service interruption or disaster.

Hosted Solutions

Recording jurisdictions may choose to have their LRMS vendor or a third-party host the LRMS Software. A number of key considerations should be addressed in planning for this option. Reliance on the LRMS vendor or the approved third-party site can relieve a jurisdiction from the management of servers and the complexity associated with the ongoing management of hardware, operating systems, databases, and security.

When considering a hosted solution, a key to success is research into multiple areas. Whether hosted "in the cloud" or at a vendor's facility, ascertain the location of the servers and the ownership of the data on those servers. It is important to retain ownership of the data

The vendor chosen to host the solution should also meet certain criteria. For example, the vendor should be experienced in hosting LRMS or other enterprise software solutions and be able to guarantee the security of the data, servers, and facility. Ensuring the financial stability of the vendor will help ensure that data will not be lost due to the hosting facility closes unexpectedly. The vendor should also guarantee protections against unauthorized intrusion by malware, ransomware, or unscrupulous employees. This protection often can be guaranteed by following security standards and obtaining certifications.

When hosting an LRMS, the vendor should provide services just like a local IT department. The vendor should have established practices for patching the operating systems, databases, and application software at the server level as well as have operational redundancy, security incident management, and response plans at the facility level. In addition, the vendor should be able to provide a jurisdiction with metrics regarding throughput, uptime, latency, and scalability. A jurisdiction should have the ability to extract data from the remote location just as they would from an on-premise solution.

Considerations

1. Can the LRMS vendor provide a detailed list of system requirements and recommendations for safely and efficiently running the LRMS? The list should address servers, operating system, databases, and peripherals.
2. Can the LRMS vendor assist the jurisdiction in assessing the compatibility of existing equipment?
3. Does the LRMS vendor have a record of accomplishment for keeping the LRMS current on both on-premise and third party software and platforms?
4. Can the LRMS meet volume and performance needs via stress testing?
5. Can the LRMS vendor meet the security needs and goals of the jurisdiction?

Integrations/Interfaces

Recording jurisdictions continue to have increased expectations that documents and data will be transmitted and received electronically with minimum integration effort. An essential component of a LRMS is the ability to integrate with multiple vendors using documented application program interfaces (API) to transmit and receive data and images. The LRMS should provide a flexible solution that allows for quick, standardized output with other software.

When integration is needed, the LRMS vendor should provide standardized formats and communication protocols. Integrating to the API should require only minimal IT resources before the integration is ready for testing and rollout. The LRMS vendor should also have the API well documented for another vendor's use. The software should be capable of supporting:

- Vendor-specific standards:
  - API calls
  - Field names
  - Index formats
  - Protocols (Hypertext Transfer Protocol Secure (HTTPS), Simple Object Access Protocol (SOAP), Representational State Transfer (REST), File Transfer Protocol (FTP))
- API calls for any relevant data:
  - Acceptance and tracking of electronic package identifiers
  - Automated notifications
  - Automated trouble-ticketing or reporting
  - Multiple exports and imports
  - Batch requests and bulk extracts
  - Ability to auto-populate data and images from other systems
  - Status and reporting
  - Cashiering and financial data
  - Tax system integration, if needed or wanted

As a best practice, an LRMS should have the ability to integrate with multiple vendors using well-formatted and documented standardized APIs.

Some of the advantages of offering integration using an API include:

1. Platform independence: An integration process using APIs should be platform/software agnostic. Any vendor planning to integrate with the LRMS should be able to use their own framework, language, and tools to integrate with the API.

Using today's technology standards, the LRMS API likely uses SOAP or REST to communicate with other applications. These are currently the two ways to access web services. Both share similarities with the HTTP/S protocol.

2. Ease of integration: Request messages, sent via HTTP/S to the service endpoint can be either:
    a. Synchronous, where the request is serviced and the response back to the client will contain the operational outcome and any data requested by the client, or
    b. Asynchronous, where the request is queued by the service and re-requests for the outcome and data are made later. This model is used when the request may be long running, or human intervention is needed before the outcome and data are available.

3. Security: The API should be SSL-encrypted, which will ensure that all communications to and from the API stay private and available only to the receiving party. It should also provide a means of authentication ensuring only trusted parties have access to the API.

Besides these advantages, some considerations for understanding whether an LRMS can support integration expectations through an API include:

1. Suitability. The API's functionality, compatibility and accuracy against comparable software should assure that the recording jurisdiction will be able to share land record data with vendors and customers, as needed, without significant additional expense or hired expertise.
2. Scalability. Can the LRMS API scale and handle multiple integrations and bulk data requests efficiently or will it fail under heavy traffic?
3. Security. Before use, make sure the LRMS vendor can validate the security of SOAP or REST transactions, without additional costs or software.
4. Documentation. The LRMS should have documentation available for vendors that provides the Extensible Markup Language (XML) formats required for submitting and communicating securely with the API.
5. Testing. A test environment is important as it allows the integrating vendor to test the application, integration and transactions using an API without affecting a live production site.

Considerations

1. Does the LRMS have a standardized data format facilitating API integration opportunities?
2. Does the LRMS have a fully functional production API that is already in use by third party vendors?
3. Is there a test environment available for use when needed?
4. What is the uptime guaranteed by the LRMS vendor?
5. Is the API integration process documented by the LRMS vendor?
6. Does the LRMS vendor provide ongoing support and management of the API?
7. Does the LRMS vendor provide certification and validation for third party vendors submitting data and images into the LRMS system?

Internet Availability

The ability to connect to the internet is an absolute minimum requirement for an LRMS. The internet is a large web of connections and access points managed by Internet Service Providers (ISP) used to connect to the World Wide Web. Once a computer is internet capable, a common naming system is used to map website addresses to Internet Protocol (IP) addresses. In addition to each computer having a unique IP address, each server address is unique. A server manages a network of computers within a specific organization.

As long as the recording jurisdiction has internet access, the connection requirements include a computer, a working internet line, the right modem for the specific type of internet line selected, and software such as internet browsers and other applications. The internet provides access to service applications such as email, web browsing, file transfer, messaging, data and image sharing, and many other interfaces. Often these applications will be incorporated into, connected seamlessly to, or provided as an add-on to an LRMS to increase the software's capabilities.

As a best practice, a recording jurisdiction should have internet connectivity as a minimum LRMS component.

Type of Connectivity

There are many ways to connect to the internet but options may differ based on available services in the area. Local service providers can offer options for connectivity in a particular area. There is no universal way to connect to the internet, but some of the most common services are Digital Subscriber Line (DSL), cable, fiber optic, broadband, satellite, and wireless. Additional information about each of these service types will be available from local internet service providers. The LRMS should be able to work within the protocols established by the local internet service provider.

Service Disruptions

Service disruptions that cause the internet to become inaccessible for extended periods should be included within any jurisdiction-wide Disaster Recovery and Business Continuity Plan. The recording jurisdiction should have written guidelines to keep interested parties apprised of service disruptions. The guidelines should also address how recording workflow will be handled during internet disruptions.

As a best practice, the recording jurisdiction should have written guidelines for handling and communicating service disruptions.

Internet service is fairly stable but there are times when services might be down for an hour or more. Recording jurisdictions which offer internet-based services, such as eRecording, online searches, or data and image downloads, will need to have a plan to handle extended disruptions. Some items to consider when planning for internet outages include:

- Notifying vendors and customers. If an outage will be longer than a few minutes, it is important that notifications be delivered in the most effective way available.
- Audit and control abilities. Once the internet connection is restored, the LRMS should provide audit capabilities to assure data integrity, such as duplicate or missing data or documents.
- Avoiding duplications caused by transmission errors. Duplicate recordings can occur when transmissions are momentarily interrupted. The LRMS should be able to monitor transmissions to avoid duplications.
- Queuing documents from vendors. The LRMS should provide a way to hold images and data for the recording jurisdiction, until service is restored, while maintaining the timing of the deliveries and the details for each package being delivered.

As a best practice, the LRMS should be able to monitor transmissions and easily audit queues to avoid duplications or corrupted data in the case of an internet service outage.

Considerations

1. Does the office have reliable and secure internet access?
2. Does the office have a communication strategy to notify vendors and customers in case of an internet service disruption?
3. Does the LRMS have safeguards to prevent errors due to an internet service disruption?

Data and Image Conversions

Conversion to a new LRMS will require planning and coordination between the recording jurisdiction's IT team and the vendor. Since many systems have multiple databases, as well as images stored inside or outside the database, this information should be conveyed to the vendor before the conversion process begins. There are multiple options when choosing the number of years and the amount of data and images to be converted from other systems. Cost and frequency of use may be factors that would limit a full and complete conversion.

As a best practice, an LRMS should have the capability to accomplish full data and image conversions and offer the ability to convert historical files incrementally as needed.

Files to be converted often have had personally identifiable information (PII) redacted. Prior to conversion, the redaction method used (burned or overlay) must be considered to avoid loss of metadata relating to the redaction. Historical files may have images with very little associated index data. Conversions may need to accommodate multiple identification numbers, including book and page number, instrument number and parcel identification number (PIN). When multiple databases are consolidated into one new database, there should be a unique identifier for each document. These identifiers are important to transfer information and should be carried forward or archived in such a way that information can be easily validated. This validation is especially essential if a data discrepancy surfaces after implementation. Determine the best conversion path for images and index data to maintain consistency throughout the process.

Conversion should follow a detailed plan such as:

- Conversion Schedule – establishes timelines for work phases
  - Initial Phase (historical)
  - Secondary Phase (gap data)
  - Final Phase (as needed)
- Conversion Location – determines where the conversion occurs
  - Vendor site
  - Recording jurisdiction site
  - Hosted facility site
- Conversion Validation – recommends testing to validate conversion accuracy
  - Record count comparisons
  - Report reconciliations
  - System configuration comparisons
  - Sampling use cases
  - User feedback
  - Parallel testing

- Conversion Anomalies – identifies conversion errors
    - Analysis and corrective steps
    - Remedial interaction by jurisdiction and vendor

Considerations

1. Can the LRMS vendor provide a detailed conversion plan that uses consistent methodology for the conversion of all data and images?
2. Can historical data be converted and easily added to the LRMS after implementation?
3. Can testing of converted data be done on site by the recording jurisdiction in a test environment prior to moving converted data to the production environment?
4. Can both non-redacted and redacted documents be converted?
5. Can images be stored outside the database post-conversion, if preferred?
6. Can the recording jurisdiction receive assistance from the prior vendor if images are stored in a proprietary format?
7. Can the LRMS vendor convert existing financial data?

Document Management

An essential component of an LRMS is document management that provides various methods of capturing and securely storing documents. Documents, once captured and indexed, should be available for searching, distributing, and storing.

Document capture is the process of introducing documents or records into the LRMS. It can be accomplished through the conversion of paper documents using scanners or through eRecording. Other ways of introducing documents to the system include importing previously digitized documents and utilizing a program that captures printed output and converts it into images for storage in the LRMS. Document management also accommodates storing electronic documents in TIFF, PDF or PDF/A, and launches the appropriate application required to view the document.

As a best practice, images should be captured in an industry-standard, non-proprietary file format with seamless integration.

Indexing is the process of extracting information from the images to easily locate the document. Most systems come bundled with the basic tools required to key metadata or to extract data, as desired. Refer to "Data Capture/Entry" (page 21) for additional information.

Search, Retrieval, and Distribution allows documents to be searched and displayed for viewing after data capture and indexing. A database is used to store indexed data and a front-end interface is provided for locating records. The ability to print, email, import/export, create reports, and publish documents from the desktop or network should also be included. Refer to "Searching" and "Data Output (Reports/Exports)" (page 37) for additional information.

Workflow is the process of moving documents from person to person or from function to function within the system, either manually or based on business rules. Refer to "Workflow" in this publication's "DAILY OPERATIONS" section for additional information.

Storage and Archive is the process of preserving the documents, images, and records captured. The LRMS should provide tools and technologies specifically required by records custodians. Refer to "Preservation" for additional information.

Considerations

1. Is the LRMS flexible enough to accommodate the office workflow and local terminology?
2. Is the LRMS scalable enough to support future growth?
3. Is the LRMS easy to use and administer?
4. Does the LRMS accommodate easy import/export of data and images?
5. Does the LRMS support capture and transfer of documents from remote locations?

6. Does the LRMS provide the ability to restrict access to certain document types per jurisdiction business rules?
7. Does the LRMS include backup or image storage options (onsite and remote)?
8. Are eRecording interfaces in place?
9. Is custom programming capability available from the vendor in order to add or modify functionality crucial to the recording jurisdiction's workflow?
10. Can the recording jurisdiction change its workflow later?
11. Are the functionalities comprehensive enough to meet the jurisdiction's needs? These may include the following capabilities:
    - To append, insert, and replace pages at capture, as well as when committed to the LRMS
    - To annotate and redact information from images
    - To provide audit trails that track when documents are altered, by whom, when and why
    - To recognize barcodes
    - To email documents
    - To provide for full text index and search

Security

The security and integrity of the LRMS should be part of the system evaluation, implementation and ongoing support and maintenance.

Typically, the jurisdiction's IT department in conjunction with the LRMS vendor shoulders the responsibility for security. Clearly defined roles and responsibilities ensure the ongoing performance of the LRMS. The LRMS vendor and the jurisdiction must work closely together to guarantee that appropriate patches, updates, refreshes, configuration, optimization, data maintenance, protection, and backups are routinely applied.

Guidelines for ensuring security can vary based on the type of LRMS integration utilized. These guidelines should be defined by the LRMS vendor and vetted by the jurisdiction's IT department. The ability to allow or restrict access to the LRMS data or infrastructure should be carefully considered prior to implementation. Data transfers between users and the LRMS should be protected against viruses, malware, key logging, ransomware, and other unauthorized intrusion. Establishing guidelines for user access, password protection, virus definition updates, and secure transmission of data are critical.

As a best practice, the ongoing maintenance of the LRMS should include a detailed security plan. The jurisdiction and the LRMS vendor should work together to ensure that the data and infrastructure remain accessible yet protected.

Considerations

1. Can the LRMS protect data against manipulation and scraping?
2. Does the LRMS protect the production database and server from external exposure?
3. What are the LRMS guidelines for user access, password protection, virus definition updates, and secure transmission of data?

Preservation

Across the United States, real property documents are considered permanent by statute, administrative code or retention schedule. This mandate means the documents in the custody of the recorder need to be accessible and reproducible forever.

Recorders initially transcribed early recordings onto paper. In time, microfilm became the preferred solution. Today electronic images with metadata are the preferred format for accessing and storing documents. These images are accessed by the public and integrated into private sector applications.

The foundation of preservation begins with capturing a quality image. The LRMS should include the capability to capture a minimum 300 DPI resolution for a TIFF image. Scanning resolution is the physical size of the picture elements (pixels) that capture the information on a page. Contrast, which is the relative difference between the background and foreground in an image, should be managed to provide the greatest degree of legibility.

PRIA advocates the principle of "layers of insurance" when considering a records preservation strategy. The ability to export images and metadata to multiple media is an example of this strategy. Paper and film are proven media and well understood technologies for archiving historical records. With continued emphasis on electronic information, both paper and microfilm are in danger of becoming obsolete for records preservation. Assuring the longevity of electronic media is a challenge for the future of LRMS.

See PRIA's Electronic Records Preservation White Paper for more in-depth information.

As a best practice, an LRMS should enable the generation of additional copies of images and metadata including export to other media, along with backup and disaster recovery capabilities.

Considerations

1. Does the LRMS vendor recognize and recommend different protocols for backup, preservation and disaster recovery of records?
2. Does the LRMS support easy export methods to enable "layers of insurance" for records preservation, regardless of the specific media?

Disaster Recovery

Service interruptions or disasters can occur in any jurisdiction. Disaster Recovery Planning and Business Continuity Planning should be incorporated in the planning process. While LRMS vendors may offer tools and recommended business practices and procedures, ultimately the responsibility remains with the jurisdiction. Planning should be closely coordinated with the jurisdiction's overall disaster recovery and business continuity efforts. Testing and verification of Disaster Recovery and Business Continuity plans are essential to expose flaws and to ensure that those plans are reliable.

It is important to assess the LRMS vendor's ability to partner with the jurisdiction in restoring service to the customer base in a prompt, efficient and cost-effective manner.

Areas to discuss and document with the LRMS vendor:

- Key contacts for each party responsible for implementing the recovery plan
- Each party's responsibilities and priorities. The jurisdiction-wide disaster recovery plan usually includes multiple layers, some of which may need to occur prior to restoring the LRMS system
- Onsite and offsite recovery capabilities and options
- LRMS backup procedures
    - Frequency of data and images
    - Redundancy, including methods and media
    - Backup storage locations, offsite and onsite
    - Testing of backups to ensure sustainability
- LRMS recovery procedures
    - Restoration sequence of software, data, images
    - Business continuity during recovery
    - Post-recovery integrity testing
- LRMS post-recovery procedures
    - Regularly scheduled review
    - Updates and testing

While no one expects a disaster, planning for one is an important part of the recorder's job. The ultimate goal is to restore service to the customer base promptly and a thorough plan is critical to an efficient recovery. The ability to recover data, equipment, and documents quickly, efficiently, and inexpensively is a big consideration when discussing new technology with an LRMS vendor.

As a best practice, recording jurisdictions should have well documented Disaster Recovery and Business Continuity Plans that include testing protocols and regular updates.

Considerations

1. How can the LRMS vendor support the recording jurisdiction's Disaster Recovery strategy?
2. Are there hardware and server configurations to implement an onsite disaster recovery plan?
3. What are the media backup types?
4. How will personnel be contacted in the event of a local disaster?
5. What is the process for system testing after a disaster to assure recovery?
6. Where is the offsite data center and what are the security certifications for that center?
7. Does the LRMS work with the jurisdiction's disaster recovery architecture?
8. How often and how are backups tested?
9. Does the LRMS assure that data is not lost if backups are done only daily?
10. Has the jurisdiction determined the acceptable loss level for data and images, and communicated that with the LRMS vendor?
11. Does the LRMS vendor offer guidelines or services for disaster recovery and business continuity?
12. If using a vendor-hosted solution, does the vendor have Disaster Recovery and Business Continuity Plans that correspond to the requirements of the jurisdiction?

DAILY OPERATIONS

Workflow

Analysis and planning are essential steps to determine the most efficient and effective workflow to meet the needs of the recording jurisdiction. Workflow defines how paper and electronic documents move through the recording office. The size of staff, document volume, and local business rules will necessitate different types of workflows. The system should allow recording supervisors to determine easily where backlogs may be occurring in the workflow so adjustments can be made as needed.

An LRMS must also be able to track all paper documents received for recording that are delivered by regular mail, express mail, or courier. Document return information should be included with the initial recording information entered into the LRMS, and the ability to print return mailing labels should be an option for the recording jurisdiction. Repetitive information, such as contacts, should be stored in the LRMS so data fields can be automatically populated.

As a best practice, an LRMS should include workflow to expedite the recording process making it as efficient as possible. The system should prompt the user for next steps and auto-populate as many data fields as possible.

Typically, mid-to-large size volume recording jurisdictions will also use a queue system that allows documents to move easily through the recording workflow. Queues will include linear processes such as document review, scanning, indexing, cashiering, verifying, and eRecording. Additional queues should provide the ability to suspend or hold documents that require additional attention or information before returning to the normal workflow. Workflow queues will vary greatly depending on jurisdiction preferences, recording volume, and size of staff.

As a best practice, an LRMS should offer the flexibility to structure workflow queues per the recording jurisdiction's preference and needs, as well as having the capability to easily deactivate (hide) or combine processes within the same queue, if desired.

Indexing and cashiering queues usually follow one another or are combined within the workflow, followed by the index verification queue. Indexed data would automatically flow to the verify queue. Scanning is a process that allows the recording jurisdiction to have the most flexibility of placement within the workflow. Documents can be scanned first with all other tasks using the image for information, or scanning can be a centralized process after cashiering and indexing and prior to

verification. Centralized scanning is usually preferred by counties with large multiple batch scanning requirements. A quality control queue would immediately follow centralized scanning.

As a best practice, an LRMS should offer the options of scan-first and centralized scanning so the recording jurisdiction can have the most flexibility in establishing workflow or revising workflow, if beneficial at a future date due to recording volume, staff, or location changes.

All images from paper documents, and usually from electronic documents, will flow through the verify queue. The LRMS should offer the option for either key-verification or sight-verification. Typically, recording jurisdictions will post recorded documents to the public web site with an "unverified" status. Once the document clears the verify queue, the designated status automatically changes to "verified."

As a best practice, an LRMS should have the flexibility and capability to allow options for the verification process.

The LRMS should accept electronic documents into a specific eRecording queue for initial review and acceptance or rejection by recording jurisdiction staff. When accepted, electronic documents should follow a similar process to that used for paper documents. Recording jurisdictions should also have the option of accepting eRecordings in a "lights-out" transparent mode with no staff review. Fee payments and posting are systematic. This advanced process usually only occurs with simple one-page documents and regular daily or weekly submittals.

As a best practice, an LRMS should have the flexibility and capability to allow recording jurisdictions to decide on the specific processes they prefer to use for eRecordings and then be able to revise the processes later, if desired.

Additional services such as issuing or recording Marriage Licenses, Passports, Birth Certificates, or Death Certificates are required by some recording jurisdictions. The LRMS should be able to accommodate these services within the core system, and the workflow should be similar with the same look and feel as recording. State legislative actions may change recording requirements; therefore, capability for these revisions should be considered.

Due to cost or time constraints, recording jurisdictions will often need to implement a new LRMS without completing the conversion or indexing of all historical records. If historical images and data are added to the LRMS at a future date, the indexing and verification should be easily accomplished. Once historical records are added to the LRMS, they should be available for public searching, the same as all other documents.

As a best practice, an LRMS should offer the recording jurisdiction the capability to add additional services in the future, as well as the capability to complete any back conversion or posting of historical records. The recording workflow should not be affected by these additions.

Recording jurisdictions should consider having an additional workflow option for the automated process of supplying both paper and electronic certified copies of recorded documents, as permissible by law. The process could occupy its own workspace or be a part of the internal and external search functionalities. Fees for certified copies should be integrated with and handled in the same manner as other recording fees. The certification stamp should be stored in the LRMS database, easily configured, and applied automatically to the document image when the certified copy is created, as either a paper or electronic copy.

Consideration should also be given to an electronic verification process of the eCertified copy. The LRMS should provide an eVerification process within the infrastructure of the LRMS or by integration with a third party.

As a best practice, an LRMS should provide the capability of automatically creating certified copies of recorded documents, both in paper and electronic formats, where permissible by law. The LRMS should also offer an option for an automated electronic verification process of the eCertified copies.

Considerations

1. Can the current recording workflow be streamlined to eliminate unnecessary or redundant steps?
2. Can paper touchpoints be decreased or eliminated?
3. Can the present office and desk floorplan accommodate an efficient recording workflow?
4. Can the workflow handle the current recording volume, and adapt to future growth years?
5. Can the workflow offer customers over-the-counter full service, as well as document batch handling through a queue system?
6. Can the workflow be easily modified by the recording jurisdiction without vendor intervention?
7. Can recording processes within the workflow be combined or hidden, if not needed?
8. Can the workflow easily accommodate seamless eRecording?
9. Can the established workflow operate simultaneously in multiple office locations?
10. Can historical document conversion and indexing be added to the LRMS without interruption of current workflow?
11. Can additional services assigned to the recording jurisdiction be added to the LRMS without interruption of current workflow?
12. Does the LRMS provide for paper and electronic certified copies?

Data Capture/Entry/Verification

Data capture is the process by which information is introduced into the LRMS. Data fields identified in statute and by policy need to be included in the LRMS. As this data is used to locate the public record, the quality of data captured in the LRMS is critical.

The LRMS should offer multiple methods of data capture, including integrated, stand-alone and automated. The method of data capture is determined by the recording jurisdiction so it is important to understand each option as data capture methods may change periodically.

Integrated data entry means data will be keyed directly into the LRMS by jurisdiction staff. LRMS systems should offer integration capabilities to obtain data (e.g., parcel identification number) from other county sources, as well as offering short cut keys, hot keys, and drop-down menus. Designated users should have the ability to edit the index data tables or the index metadata independently or with the assistance of the vendor.

Stand-alone data entry means that the jurisdiction staff will key required data points in a separate module outside of the LRMS or it might include outsourcing to a third party. That information is then transmitted back to the LRMS as a pass-through.

Automated data capture means the manual keying duties are replaced with either an integrated or stand-alone module. Automated data capture will be either knowledge-based or rules-based.

- Knowledge-based data capture technology begins with an initial document sample set, with index values representing what data should be pulled from the document and in which fields the data should be placed. Optical Character Recognition (OCR) is used to identify the sample set. The technology should review data from production and refine the knowledge base over time to maximize accuracy.

- Rules-based data capture requires uniquely identifiable forms where the data lies in specific pre-defined locations (such as IRS liens). This technology uses a small sample set of documents. As documents change, the rules must be modified to accommodate any documents affected by the change.

A partially automated data entry option is called rubber-banding or roping. This type of OCR involves the ability to draw a box with the mouse around a section of data, capturing text from within the drawn box inside a scanned document, and placing it into an index field.

Although automated data capture can streamline and simplify data entry efforts, the jurisdiction should assure the LRMS provides the ability to disable the functionality.

Data capture fields should be configurable to reflect local terms, index requirements, references, and rules. The jurisdiction should have the option to designate required fields. The formatted data captured from electronic documents, automated entry, and keyboard entry should be consistent.

The LRMS should also provide a way to verify data integrity. Methods include sight verification and blind key verification:

1. Sight verification involves comparing the screen containing data initially captured or keyed against the image of the recorded document on a monitor, and manually keying corrections as needed.
2. Blind key verification involves manually keying data viewed on the image into empty data fields. Ideally, the person blind keying was not involved in the initial capture. The LRMS compares the re-keyed information to the original and should alert the user when the data entered does not match what was previously entered. Options should be available to remedy discrepancies. The recording jurisdiction may specify fields to be blind key verified.

The LRMS should provide an audit trail of any modifications made during data capture and verification. Audit trail information should be viewable in multiple formats to identify training needs and monitor quality control.

As a best practice, an LRMS should include blind key verification capability, which commonly is viewed as the most effective method of finding errors.

The LRMS should link any document to any other related document (release to lien), and in multiple formats (document number to book and page).

Considerations

1. Does the LRMS support multiple methods of entering data?
2. Can automated data capture be disabled, if used?
3. Does the LRMS allow configurable database fields and tables?
4. Is it possible to designate required fields?
5. Does the LRMS support the ability to link related documents, such as mortgage and assignment, along with multiple fields such as document number to book and page?
6. Does the LRMS include the ability to sight verify and blind key verify?
7. Does the LRMS restrict the ability to modify data based on user security configurations?
8. Does the LRMS include data modification alerts, audit trails, and reports?
9. Does the LRMS interface with other county sources to reduce or eliminate redundant keying?
10. Does the LRMS offer time saving features such as short cut keys, drop down menus or hot keys?

Receipting

The receipting function of an LRMS should allow a recording jurisdiction to collect fees, receive payments, generate endorsements, and manage administrative controls while seamlessly interfacing with the rest of the system. Each LRMS may employ different processes for filing and recording documents, and should allow equivalent functionality for all delivery methods, whether physical or electronic.

As a best practice, an LRMS receipting process should be consistent for all delivery methods, whether physical or electronic.

Review of Documents

The receipting process includes reviewing the document for recordability. While this review may vary by jurisdictions, typical items reviewed are acceptable document type, the notarial acknowledgment, signatures, location of the property, and availability of sufficient funds. If a document cannot be accepted, the LRMS should include a rejection process that allows the user to correspond with the document submitter, either electronically or physically. The LRMS should also include the ability to hold or suspend a transaction in cases where additional information or funds are needed prior to accepting the document(s).

Ease of Use

The LRMS should include automated fee calculations that are table-driven based on factors defined by the recording jurisdiction. Examples of common factors include document type, page count, number of names, and number of properties. Jurisdictions collecting transfer or mortgage taxes may also require the LRMS to calculate taxes based on a consideration or loan amount. In addition to document fees, the LRMS should allow the collection of document surcharges and miscellaneous fees at the time of recording. Examples include fees for non-standard documents, document copies, certified copies, courtesy labels, or other fees unrelated to recording.

The LRMS should have the option to enter index information at the time of receipting. This entry should be consistent with other indexing processes within the system.

Collection of Fees

The cashiering function of an LRMS should allow for multiple tender types, including but not limited to: cash, check, draw-down account, credit account, ACH, credit card, and journal entry. It is recommended that the system alert for shortages, overages, and provide for refunds.

Endorsements

The LRMS system should have a method of endorsing documents with the recording and filing data that is consistent between physical and electronic documents. The endorsement should include the primary identification number, date and time recorded, jurisdiction name, document type, and fees collected. Individual jurisdictions may include additional information at their discretion. Endorsements may be applied in multiple ways such as a printer, receipt printer, label, or digital stamp.

Overrides

The receipting function should include the ability to override the fees with supervisory approval. Overrides are typically based on statute, regulation or jurisdiction policy and should be applied on a case-by-case basis. Examples of overrides in receipting include adjusting fees collected or waiving the fee on a single document or the entire receipt. Receipting and override functions should be audited by the LRMS to allow the jurisdiction to track all financial activity.

Adjustments

An LRMS should accommodate adjustments to receipts when an error has been detected. The most common reasons for issuing a receipt adjustment include:

- Incorrect payment or tender type
- Incorrect document type
- Incorrect page count
- Incorrect transfer tax

The adjustment process should provide a jurisdiction with the ability to issue a new, corrected receipt and accommodate adjustments to the amount collected. LRMS vendors should work with jurisdictions to determine how such adjustments are to be handled on the same day or in instances where the adjustment is made one or more days after the initial transaction. The LRMS should include the ability to restrict receipt adjustments to supervisory personnel and should provide an easy means of auditing adjusted receipts.

Voiding Receipts

In some instances, jurisdictions may require that a receipt be voided. Reasons for voiding a receipt may include the withdrawal of a recording request by a client, duplicated recording, or the discovery that the recorded document belongs to a different jurisdiction. Voiding receipts should be based on the specific policy of the jurisdiction. The LRMS should restrict the voiding of receipts to supervisory personnel and should provide an easy means of auditing voided receipts.

As a best practice, an LRMS should include an audit feature that tracks and reports all receipt modifications including overrides, adjustments, and voids.

Managing the Cash Drawer

The LRMS should include a method to account for a cashier's money intake. This accounting includes managing the starting cash on-hand, tracking overages and shortages, and registering all tender types taken. The LRMS should allow a user to open, close, and balance a cash drawer at any time. The system should include reports and functionality to allow users to determine readily the amount expected for each tendered type.

The system should include the ability for only supervisory personnel to balance multiple cash drawers. If required by the jurisdiction, this ability may include balancing cash drawers in multiple locations. The system should produce reports that supervisory personnel can use to ensure that each cash drawer is balanced on a daily basis.

Fee Maintenance

Recording fees are subject to change at any time. LRMS software should allow the staff of a jurisdiction to establish new fees, update existing fees, or retire fees, with or without vendor support and prior to the effective date of the change. A table-driven approach would allow supervisory staff to modify fees quickly and easily by updating the tables on which those fees are based. The LRMS should retain information relating to older, obsolete, or retired fee schedules, as well as have the ability to accept documents using those fee schedules, as needed.

As a best practice, an LRMS should allow modifications to the fee tables.

Considerations

1. Does the LRMS support multiple tender types?
2. Can Supervisors modify or void receipts?
3. Does the LRMS itemize individual components of the recording fee, if needed?
4. Can the LRMS restrict access to cash drawers via rights and roles?
5. Does the LRMS allow supervisors to balance any drawer, as needed?

Scanners/Scanning

Scanning is a common method used to add documents, either directly in the recording jurisdiction office or on the submitter's side if eRecording. Scanners convert paper documents into digital images.

These digital images can then be used in lieu of the paper throughout the recording process and for storage and retrieval in an LRMS.

As a best practice, an LRMS should offer seamless integration between the scanning component and other LRMS components.

Scanner Selection

LRMS vendors can assist with the selection of a new scanner or verify if an existing model is compatible with the new software. A wide variety of scanners and price points exist. Selection considerations should be based on the features required to accommodate recording volume and workflow in addition to any other paper that will be captured in the office(s).

Select the best fit from these Standard Scanner Options:

- Scanning speed: simplex pages per minute (ppm) or duplex images per minute (ipm)
- Daily Duty Cycle: the maximum number of pages recommended
- Resolutions supported (minimum 300 dpi)
- File format and compression choices such as monochrome, grayscale, color, TIFF, PDF
- Auto Doc Feed (ADF) and/or Flat Bed
- Maximum/Minimum document size (letter, legal, 11 x17, specialized scanners for maps and plats)
- Drivers/Interfaces supported: USB, SCSI, TWAIN, specialized drivers for map scanners
- Quality control assistance such as double or multi-page feed detection, blank page detection, automatic document size detection, color dropout, rotate page
- Warranties and service options available

As a best practice, an LRMS should capture images in industry-standard, non-proprietary file and compression formats. TIFF image resolution should be a minimum of 300 dpi.

Scanning Process

- Pre-Scan Preparation
    - Remove all staples, paper clips, and unfold the pages. Consider using the flatbed if pages are torn.
    - Insert document separators if applicable such as barcode or blank pages.

    - Verify that all parameters are configured correctly. These parameters can include, but are not limited to, file format, resolution, paper size, color dropout, paper source (flatbed or ADF), simplex or duplex.
- Scan and Post-Scan
    - Recognize the scanner's capabilities and limitations (e.g., overloading paper in the ADF can cause jams and rips).
    - Use the scanner's available tools to assist with quality control such as multiple page feed detection, automatic size detection, automatic rotation, deskewing and despeckling.
    - Verify all pages were scanned and are legible.
    - Verify all documents are complete.
    - Use scanner or LRMS tools such as insert, replace, append or reorder pages or batching to make necessary modifications.

LRMS Workflow Options Post Scanning

Most scanners ship with software programs such as image capture, OCR, barcode and image enhancement tools such as deskew and despeckle. Check with the LRMS vendor before installing any software. Typically, the LRMS is already integrated with tools specifically designed to use with land records in recording jurisdictions. Examples include:

- Auto split on patch/bar code
- Barcode interpretation of key field(s)
- Full text OCR or Auto-index
- Redaction
- Image and data export for archival, consumers, or filming

Considerations

1. Which scanners are compatible with the LRMS?
2. Will the scanners and LRMS accommodate all document sizes and characteristics?
3. Do the scanners offer cost effectiveness with image quality, speed and reliability?
4. Are maintenance parts for the scanners such as cleaning kits, pads and pick rollers, available and affordable?
5. Does the manufacturer warranty and service options for the scanner meet the office's requirements and budget? Options can include shipping to service center, onsite coverage, and exchange unit replacement programs.
6. Will the scanners accommodate short term and long-term needs?
7. If leasing scanners is an option, is it a better fit than purchasing?

eRecording

The ability to receive and process documents submitted electronically is a basic requirement of today's LRMS. eRecording is the process of receiving, reviewing, recording, and returning electronic documents. If documents are not recordable, the electronic document is rejected by the recording jurisdiction back to the submitter with a rejection reason. Submitters can then correct and resubmit the electronic document. When enabled to eRecord, a recording jurisdiction can process and record digital documents while mirroring the workflow used to record paper documents.

There are two types of electronic documents that may be presented for recording. One type is images that originate as paper documents, then are scanned and submitted electronically. The second type is fully electronic and has been digitally signed and notarized. Documents are typically submitted to the recording jurisdiction by an eRecording vendor. These vendors usually integrate with the recording jurisdiction's LRMS to submit seamlessly electronic documents and data for recording. The vendors have submitter customers who are trained to use the vendor's software to expedite the electronic delivery of recordable documents into the recording jurisdiction. There is also the option for government-to-government (G2G) integrations to streamline interagency recordings.

With these submission types there can be some preliminary identifying data provided for streamlined recordation. The digital documents are delivered to the recording jurisdiction as either TIFF or PDF images, based on the recording jurisdiction's preference. Once these electronic documents are recorded, they can be seamlessly inserted into the LRMS without having to be scanned first and uploaded into the paper workflow.

As a best practice, an LRMS should provide seamless integration between the handling of electronic documents and paper documents to simplify the recording workflow.

The LRMS should provide a flexible workflow for recording both paper and electronic documents so the recording jurisdiction can manage one consistent recording process. Flexible workflow should, at a minimum, allow the recording jurisdiction to:

1. Receive, view, modify, and handle fee discrepancies so that fee information received from the submitter can be compared to fees charged by the recording jurisdiction. The recording jurisdiction should be able to notify the submitter that the estimated fees and actual fees vary, prior to recording, rather than trying to resolve discrepancies after the recording has been completed and paid for.
2. Review and edit identifying data delivered by the submitter.
3. Allow for data entry or review of identified data. A recording jurisdiction may have unique indexing data requirements so the ability to add, modify, identify or delete information quickly and efficiently will accommodate jurisdiction-specific requirements.

4. Minimize and standardize document types to support simpler naming conventions across multiple recording jurisdictions.
5. Change the document type selected if the submitter has inaccurately named the document type based on the recording jurisdiction's naming conventions.
6. Use standardized rejection reasons for both paper and electronic documents.
7. Add new submitters into the LRMS quickly and easily.
8. View comments provided with the submission to minimize rejections or incorrectly recorded documents.
9. Receive and track electronic package identifiers needed when package questions arise. Identifiers can be used to safeguard against duplicate recordings by providing alerts to warn the recording jurisdiction if newly received documents and data match previously processed recordings. These safeguards also enhance the ability to troubleshoot discrepancies between the recording jurisdiction and electronic document submitters.
10. Accept and process supporting documentation. Support documents are not recordable but are needed to communicate recording expectations. These documents can assist the recording jurisdiction in reviewing and correctly assessing the recordability of documents without these support documents becoming part of the public record.

As a best practice, an LRMS should process paper and electronic documents using a similar workflow so the recording process for electronic documents is no more complicated than the recording process for paper documents.

To assure that eRecording is merely another way of delivering documents into the LRMS for review and recording, the recording jurisdiction needs to have accurate accounting of both electronic documents that are recorded and the fees and payments for those recordings. Basic reporting capabilities for eRecording include:

1. Robust reporting for daily batch payments (ACH) from the eRecording vendors.
2. Daily reports indicating documents submitted, recorded, and rejected. The recording jurisdiction should be able to create consolidated reports for all recordings, as well as reporting on eRecording separately from paper recording.

Refer to "Data Output (Reports/Exports)" for additional information.

The concept of a flexible workflow in the LRMS means the recording jurisdiction can simultaneously work with paper and electronic documents while keeping control over the recording process. LRMS vendors can assist with simplifying the receipt and handling of electronic documents by assuring that the recording workflow can incorporate paper and electronic documents into one recording process.

Considerations

1. Does the LRMS accommodate the delivery, acceptance, and return of electronic documents?

2. Does the LRMS support eRecording by making it at least as efficient as the paper recording process?
3. Can staff make changes as needed without returning the transaction to the submitter?
4. Does the LRMS provide an efficient method for rejecting transactions?
5. Does the LRMS have the ability to display an electronic signature and notarization?
6. Can all document types accepted by the jurisdiction be eRecorded?
7. Can the LRMS route electronic documents to other local and state agencies required by the jurisdiction as part of the workflow process?
8. Does the LRMS allow a submitter fee tolerance to assure that both the submitter and receiver agree on the recording charges prior to recordation?
9. Can the submitter send notes for review, related to a specific document or package?
10. When an eRecorded document is modified after recordation, does the LRMS notify the submitter?
11. If there are communication interruptions during delivery, does the LRMS recognize and respond to the error?
12. Does the LRMS have safeguards in place to prevent duplicate recordings when documents are electronically delivered?

Redaction

Redacting Personally Identifiable Information (PII) from public documents recorded in the LRMS should be done when required by state, county or city legislation, or office policy. Internal county departments, lenders, title companies, or other stakeholders should be consulted about the proposed policy before it is implemented in an effort to minimize unintended consequences. Another consideration for the policy development is whether bulk data customers and copy requestors receive redacted or un-redacted images.

As a best practice, redaction policies and procedures should be based on local rules and statutes, and take into consideration the impact to anyone using the public record.

After the policy has been finalized, the LRMS vendor should be provided with rules for redaction such as redacting only the first five digits of the social security number, all driver's license numbers, or dates of birth. The rules should reflect mandated requirements; however, the ability to redact, when needed, should be a minimum requirement of an LRMS.

Some key questions that should be answered about the redaction process by the jurisdiction and the LRMS vendor:

- Will redaction be done manually by staff or automatically by the LRMS?
  - If the redaction will be done manually by staff, at what stage of the process will the redaction occur?
  - Who on the staff will be allowed to redact?
- Will the redaction be done automatically?
  - Will all documents be screened for PII candidates?
  - Will there be any manual review by staff for accuracy?
  - If so, at what stage will that review happen?
  - If the redaction is being done automatically, can it be overridden if it is incorrect?
  - Can the automated redaction be shut off or disabled?

The jurisdiction may prefer to have a stand-alone module or integrated interface for redaction. Stand-alone modules typically use a separate web interface that staff will need to access and login to in order to review potential candidates for redaction. The integrated interface should be included within the LRMS. Either option should be able to provide reports that identify the number of documents reviewed and the number of redactions completed.

A knowledge-base-driven interface will need to be periodically updated as the system learns what and how information is to be redacted. Rules-driven interfaces will need to be updated as laws, rules, and policies change. Access to redaction tools in either interface should be controlled by security levels as determined by the jurisdiction.

There are typically two methods of redaction: burn or overlay. Burned redaction burns the document image with a box that covers the identified PII. Overlay uses coordinates from the document to hide the identified PII. It is important to note that the PII redacted using the overlay method may be skewed on the document during viewing, printing or any conversion process.

The LRMS should always have the capability of displaying redacted, as well un-redacted images. Regardless of which type of redaction is used, there should be some type of final review by jurisdiction staff before the image is released for public use.

Considerations

1. Does the LRMS restrict access to unredacted images?
2. Does the LRMS allow manual redaction and automated redaction?
3. Does the LRMS allow for PII to be redacted at multiple points in the workflow?
4. Does the LRMS accommodate future changes to redaction requirements?
5. Does the LRMS document the manner in which information is redacted from images?

Searching

The LRMS should provide an interface for users to enter one or more search criteria that will be formatted into a query that displays results for review.

As a best practice, the results of a search should include all records that meet or exceed the criteria.

Criteria Selection

At a minimum, the LRMS should offer the ability to search basic data fields such as:

- Recording date
- Instrument number
- Instrument type
- Party names
- Book and page

Additionally, it should support a specific method of searching each field such as:

- Exact match
- Greater than or less than
- Range
- Null or not null
- Soundex (sounds like)
- Cross name (grantor and grantee)
- Wild card searches

Search Results

The LRMS should process requested selection criteria to display results, often in a grid format. The user can view and download the corresponding images. In addition to downloading and viewing, the LRMS should facilitate image printing, emailing, faxing, and other output methods required by the jurisdiction.

Staff Efficiencies

Beyond basic search capability, the LRMS should offer methods of improving efficiency, such as the ability to:

- Perform secondary searches and append the results
- Personalize screen appearance and search options
- Secure search options such as restricting changes to the database or limiting searches to specific fields or document types
- Re-arrange or re-size windows, zoom in or out, show thumbnails

- Use dual monitors
- Rotate, insert, or append pages

Public Access

The LRMS should offer methods for the public to search records such as:

- Access to a PC or kiosk in a jurisdiction's office for the public to search, select, print and pay for documents
- Web access that enables the public to search records
- eCommerce ability for online purchase and delivery
- Access compliant with ADA requirements

Considerations

1. Do the searchable fields meet the needs of the jurisdiction?
2. Can the screens be configured based on the user rights?
3. Is the search functionality user-friendly?

Accounting

The accounting functions in an LRMS are critical to the daily operation of a recording jurisdiction. Jurisdictions have a variety of accounting needs including reconciling fees and revenues, making adjustments and corrections, and reporting.

The LRMS should have the ability to balance across multiple workstations, cash drawers, or tills at any time during the day and allow the allocation of fees collected to any number of ledger accounts. Jurisdiction staff should have the ability to adjust those allocations.

As a best practice, an LRMS should balance across multiple workstations throughout the day and be able to handle multiple tender types.

Any person receipting into an LRMS should have a unique login or identification for auditing purposes. Staff members at a specified security level should be able to close and balance cash drawer(s). In addition, as defined by security settings in the LRMS, supervisory level staff should have the ability to resolve situations where an out-of-balance condition has occurred.

In a recording jurisdiction, accounts may be established for the payment of accumulated fees. Examples include local title companies and eRecording submitters. The LRMS should allow the recording jurisdiction to determine which accounts need to be set up as escrow, deferred payments, or billable accounts. Appropriate recording jurisdiction staff should be able to adjust customer accounts. The LRMS should include a process for invoicing customers, creating and printing statements, and accommodating over and under payments. The LRMS should have the ability to integrate with the jurisdiction's primary accounting system to transfer seamlessly and efficiently all accounting data.

The LRMS should provide a variety of accounting reports that have the flexibility to compare fees charged and revenues collected, as well as current balances. These reports should include basic predefined reports, as well as the ability for the recording jurisdiction to modify or create reports to best suit their needs. Multiple file formats should be available as report output, including .txt, .xls, .csv, .html, and .pdf. Additionally, the LRMS should have the ability to produce regularly scheduled reports, as well as on-demand reports.

As a best practice, an LRMS should provide a variety of standard accounting reports, and the ability to modify or create reports to best suit the needs of the recording jurisdiction.

Considerations

1. Can the LRMS convert existing financial data from the previous system?
2. Does the LRMS allow customers to access their account information?
3. Does the LRMS support GAAP (Generally Accepted Accounting Principles) compliance?
4. Does the LRMS meet PCI (Payment Card Industry) data security standards, if the recording jurisdiction accepts credit card payments?

Data Output (Reports/Exports)

A major responsibility of the recorder is supplying information to the public and other government agencies. An LRMS should provide various export methods to allow the recorder to have the flexibility needed to meet all governmental requirements and public demands.

One of the most common means of output is running reports with variable criteria that return a set of data from the LRMS. The LRMS should provide standard reports, as well as offer the users the ability to perform ad hoc reports.

Standard reports are typically system-generated or created by report tools such as Crystal and SQL Server Reporting Services (SSRS). Examples include financial, productivity, state transfer tax, and receipts. Knowledgeable staff should have the ability to create, update, and maintain reports without reliance on the LRMS vendor. Additionally, the LRMS should include the ability to export reports in multiple forms such as HTML, text files, Word, Excel, CSV, PDF, and PDF/A.

Other reports, such as ad hoc reports, can be created on demand and should be easy to define and to adjust per the user's needs. Examples of these reports include a list of documents submitted by a specific agent, a list of active queues, or a staff productivity report. Reports may use a variety of parameters such as date range, location, system user, or document type.

Forms, which are pre-defined templates, are another widely used means of exporting data from an LRMS. Similar to reports, forms can be system generated or developed using tools such as Crystal and SSRS. Examples include generating a letter for a suspended transaction, a rejection letter, or cover pages.

As a best practice, standard reports and forms, customizable search reporting, the ability to export reports in multiple formats, and the option for staff to create, update, and maintain reports should be included in an LRMS.

The LRMS should have the capability to export data and/or images in batch or bulk mode, as well as individually or together. To easily use the exported data and/or images, the LRMS should have the ability to:

- Export data to a file directory or FTP location that meets the needs of the recording jurisdiction
- Name the indices and images by commonly used terms, such as the instrument number or book and page of the document
- Set defined parameters for the export, such as date range or document type
- Define image types and formats to be exported, such as original, redacted or PDF/A
- Schedule on-demand or automatic exports to run daily, weekly, and/or monthly

As a best practice, an LRMS should include maximum flexibility in exporting data and images so that the information is both useable and easily understood.

Web access can also be classified as a method of data output. The recording jurisdiction should decide which data and images will be fully accessible to the public or by subscription. If eCommerce is preferred, the LRMS will need the ability to handle subscription or non-subscription services, as well as payment transactions for these services.

Considerations:

1. How much control and flexibility does the recording jurisdiction need and want for creating new reports?
2. Does the recording jurisdiction have knowledgeable staff available to create or revise reports and forms?
3. What customization is available from the LRMS vendor and at what cost?
4. Can the LRMS export data and images at scheduled intervals?
5. If applicable, will the LRMS support data and image exports as a revenue source for the recording jurisdictions?
6. Can the LRMS handle interdepartmental requests for data?

THE FUTURE OF LRMS

An effective LRMS should have the ability to adapt to the changing requirements of the recording jurisdiction in the future. Similarly, it is important that an LRMS provide workflow flexibility that can adapt to the recording jurisdiction, rather than require that the recording jurisdiction's workflow be modified to fit the conceptual design of the LRMS. When evaluating the pros and cons of an LRMS, the recording jurisdiction should also consider the vendor's commitment to future innovation and the ability to migrate to new development platforms.

As a best practice, an LRMS should provide a flexible workflow that can adapt to the recording jurisdiction rather than require that the recording workflow be modified to the LRMS workflow.

In addition to a flexible workflow, the recording jurisdiction should consider whether the LRMS could easily adapt to future advances in:

- Web services
- Redaction needs
- Storage and retrieval options
- Communication protocols
- Indexing and unique document identifiers
- Export and import efforts
- Audit and control advances
- Metadata storage
- Document control
- Field format standardization efforts
- Bulk data and image uploads and downloads

Future LRMS functionalities will likely provide enhanced access to data and images within the LRMS. The public facing interaction with the LRMS will include options for the public to be able to serve themselves: searching for, ordering, and paying securely for services online. Recording jurisdictions and customers will also benefit from LRMS products that provide access via mobile apps, satellite location kiosks, and Geographic Information System (GIS) integration. Interactive functionality with other applications, as well as with public offices and private businesses, is a trend that will likely continue and will improve public access, transparency, and customer service.

Considering the importance of archival image quality for permanent property records in a digital environment, LRMS products should automatically assure that incoming images maintain minimum resolution requirements. (See Scanner/Scanning on page 26.) Additionally, evolving LRMS products should accommodate emerging file formats that support preservation.

A recording jurisdiction should be able to stay with its LRMS knowing the system is designed and ready to adapt to ongoing needs. Development of future features of LRMS products will be a collaborative effort between recording jurisdictions and LRMS vendors to meet the needs of the property records industry.

APPENDIX A: BEST PRACTICES

Section	Best Practices	Section Page
Preparation and System Planning	As a best practice, the recording jurisdiction should establish separate servers or databases for production, testing or training, and web applications. All servers should reside inside the firewall with limited open ports for external customers.	Page 2
Hardware	As a best practice, an LRMS system should include server, workstation, and peripheral hardware components that are configured to ensure the efficient operation of the application.	Page 2
Infrastructure Protection	As a best practice, an LRMS system should include protection from virus, malware, key logging, ransomware and other externally introduced threats. Additional steps should be taken to protect the infrastructure in the event of service interruption or disaster.	Page 4
Integration and Interfaces	As a best practice, an LRMS should have the ability to integrate with multiple vendors through the use of well-formatted and documented standardized APIs.	Page 6
Internet Availability	As a best practice, a recording jurisdiction should have internet connectivity as a minimum LRMS component.	Page 8
Service Disruptions	As a best practice, the recording jurisdiction should have written guidelines for handling and communicating service disruptions.	Page 8
Service Disruptions	As a best practice, the LRMS should be able to monitor transmissions and easily audit queues to avoid duplications or corrupted data.	Page 9
Data and Image Conversions	As a best practice, an LRMS should have the capability to accomplish full data and image conversions and offer the ability to convert historical files incrementally as needed.	Page 10

Document Management	As a best practice, images should be captured in an industry standard, non-proprietary file format with seamless integration.	Page 13
Security	As a best practice, the ongoing maintenance of the LRMS should include a detailed security plan. The jurisdiction and the LRMS vendor should work together to ensure that the data and infrastructure remain accessible yet protected.	Page 14
Preservation	As a best practice, an LRMS should enable the generation of additional copies of images and metadata including export to other media, along with backup and disaster recovery capabilities.	Page 15
Disaster Recovery	As a best practice, recording jurisdictions should have well-documented Disaster Recovery and Business Continuity Plans that include testing protocols and regular updates.	Page 16
Workflow	As a best practice, an LRMS should include workflow to expedite the recording process making it as efficient as possible. The system should prompt the user for next steps and auto-populate as many data fields as possible.	Page 18
Workflow	As a best practice, an LRMS should offer the flexibility to structure workflow queues per the recording jurisdiction's preference and needs, as well as having the capability to easily deactivate (hide) or combine processes within the same queue, if desired.	Page 18
Workflow	As a best practice, an LRMS should offer the options of scan-first and centralized scanning so the recording jurisdiction can have the most flexibility in establishing workflow or revising workflow, if beneficial at a future date due to recording volume, staff, or location changes.	Page 19
Workflow	As a best practice, an LRMS should have the flexibility and capability to allow options for the verification process.	Page 19
Workflow	As a best practice, an LRMS should have the flexibility and capability to allow recording jurisdictions to decide on the specific processes they prefer to use for eRecordings and then be able to revise the processes at a later date, if desired.	Page 19

Workflow	As a best practice, an LRMS should offer the recording jurisdiction the capability to add additional services in the future, as well as the capability to complete any back conversion or posting of historical records. The recording workflow should not be affected by these additions.	Page 20
Workflow	As a best practice, an LRMS should provide the capability of automatically creating certified copies of recorded documents, both in paper and electronic formats, where permissible by law. The LRMS should also offer an option for an automated electronic verification process of the eCertified copies.	Page 20
Data Capture/Entry	As a best practice, an LRMS should include blind key verification capability, which is commonly viewed as the most effective method of finding errors.	Page 22
Receipting	As a best practice, an LRMS receipting process should be consistent for all delivery methods, whether physical or electronic.	Page 23
Voiding Receipts	As a best practice, an LRMS should include an audit feature that tracks and reports all receipt modifications including overrides, adjustments, and voids.	Page 25
Managing the Cash Drawer	As a best practice, an LRMS should allow modifications to the fee tables.	Page 25
Scanners/Scanning	As a best practice, an LRMS should offer seamless integration between the scanning component and other LRMS components.	Page 26
Scanner Selection	As a best practice, an LRMS should capture images in industry standard, non-proprietary file and compression formats. TIFF image resolution should be a minimum of 300 dpi.	Page 26
eRecording	As a best practice, an LRMS should provide seamless integration between the handling of electronic documents and paper documents to simplify the recording workflow.	Page 28
eRecording	As a best practice, an LRMS should process paper and electronic documents within a similar workflow so the recording process for electronic documents is no more	Page 29

	complicated than the recording process for paper documents.	
Redaction	As a best practice, redaction policies and procedures should be based on local rules and statutes and take into consideration the impact to anyone using the public record.	Page 31
Searching	As a best practice, the results of a search should include all records that meet or exceed the criteria.	Page 33
Accounting	As a best practice, an LRMS should balance across multiple workstations throughout the day and be able to handle multiple tender types.	Page 35
Accounting	As a best practice, an LRMS should provide a variety of standard accounting reports, and the ability to modify or create reports to best suit the needs of the recording jurisdiction.	Page 35
Data Output (Reports/Exports)	As a best practice, standard reports and forms, customizable search reporting, the ability to export reports in multiple formats, and the option for staff to create, update, and maintain reports should be included in an LRMS.	Page 37
Data Output (Reports/Exports)	As a best practice, an LRMS should include maximum flexibility in exporting data and images so that the information is both useable and easily understood.	Page 38
The Future of LRMS	As a best practice, an LRMS should provide a flexible workflow that can adapt to the recording jurisdiction rather than require that the recording workflow be modified to the LRMS workflow.	Page 43