

# Pension Administration Systems: From RFP to Implementation and Beyond

By: Thomas Dover and Michelle Mellon-Werch

Pension Administration Systems (PAS) have been around for a long time, quietly keeping track of vital information necessary to administer and operate a public retirement system. These critical systems keep up with administration needs, user demands, technology challenges and legal requirements. This article seeks to inform and identify some of the critical components of a PAS procurement and how, as legal counsel, we can provide guidance and assistance to improve our retirement system’s chance of a successful outcome.

## Data Migration and Legacy Data

The core of any PAS is the integrity of the data. What is the data, where is the data and how do you access, process, and report the data? If you are considering moving to a new PAS from a legacy PAS, answering these questions and documenting them is a critical step that will require substantial staff resources.

### What is the data?

Member data in a legacy PAS typically includes personally identifiable information (e.g., name, address, birth and death dates, social security numbers), employer information, service credit, your system forms (e.g., new member enrollment, beneficiary designations, applications), court orders and historic transactions. Each data point must be mapped to the processes that use the data, reporting requirements and access rights.

### Where is the data?

Identifying the location, form, and categories of all relevant member data is important for PAS requirements and may be a challenge for systems that have an older PAS or fewer staff.

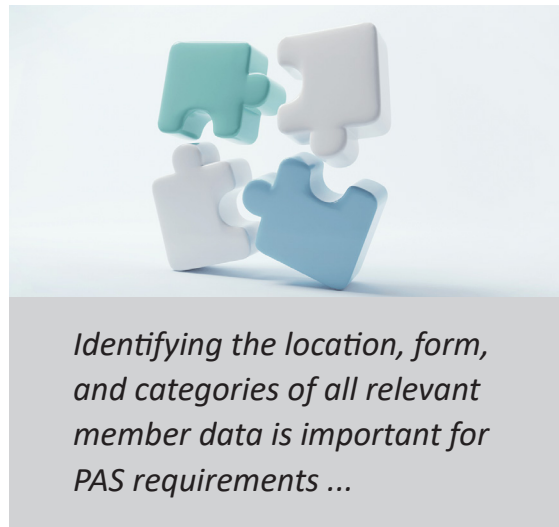
### How do you access, process, and report the data?

The answer to this question will inform how you consider data migration from a legacy system into a new PAS. The PAS will likely integrate with internal systems (e.g., finance, operations, and data security) and external systems, such as user portals and banking.

Your system may want to consider the following alternatives depending on your applicable procurement processes, regulations and state laws governing this process. You may be required to issue a Request for

Proposals (RFP) to purchase a PAS and obtain related services:

- 1) Issue an entirely separate RFP for data migration from an RFP for a PAS procurement.
- 2) Issue an RFP that combines data migration with a PAS procurement and require vendors to price independently, and combined, for data migration and PAS procurement.
- 3) Issue an RFP for a single vendor that provides both data migration and PAS services and software.



*Identifying the location, form, and categories of all relevant member data is important for PAS requirements ...*

There are case-specific pros and cons for each RFP structure but key performance indicators (KPIs) for the data migration vendor should focus on custom data mapping to the new PAS specifications, data integrity, conversion of physical records, and data cleansing.

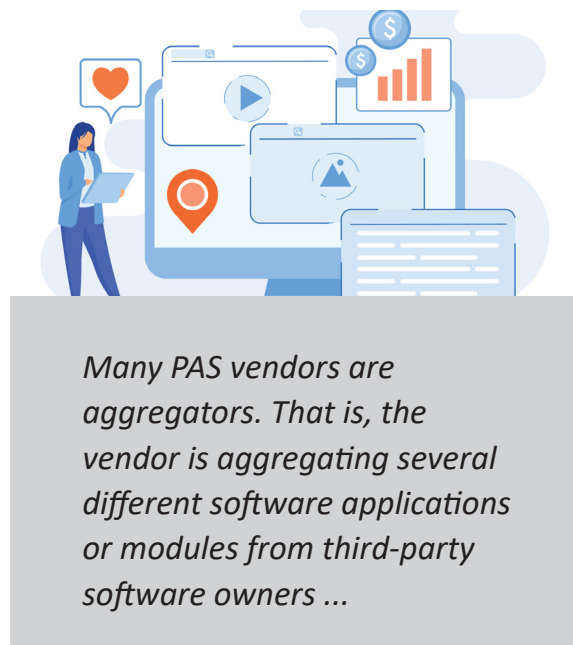
**Software and Intellectual Property (IP) Ownership and Licensing**

Software environment issues, open source, Artificial Intelligence (AI) developed software, and the complex integration of third-party software and database structures utilized by technology providers affect the methods of service delivery. It’s important to consider the effect of these technologies on PAS, regardless of how services are delivered and then address the legal and technical risks when we contract with vendors and their service providers.

Putting requirements around ownership, licensing rights and service platform options into the RFP can help raise issues with vendors before they become an implementation risk factor.

Whose software is included in both the PAS and services?

Many PAS vendors are aggregators. That is, the vendor is aggregating several different software applications or modules from third-party software owners to create a single PAS for the retirement system. Vendors that own their own software may still incorporate other software to assist with user portals, reporting or one of the many other added functionalities necessary to administer pension benefits. In the end, nearly all PAS vendors incorporate some variety of software developed and owned by a third party.



A vendor should be willing and able to identify all third-party owners whose software is:

- 1) required by,
- 2) incorporated into, or
- 3) combined with the PAS and/or the services provided in any maintenance and support obligations.

With an aggregated solution it is important to require:

- 1) the PAS contract terms apply to each third party, and
- 2) the vendor provides an Intellectual Property (IP) ownership and non-infringement representation and warranty, along with an indemnification obligation for all IP, including third-party IP.

What rights does the retirement system (or a separate vendor) have to the software?

Only the owner of software can license rights to the software and permit the subli-

censing of those rights. Once you have established who owns the rights, via proper representation and warranties, can you consider which critical rights are necessary for the PAS.

Copyright, patent, and trade secret laws provide for several different rights that are bundled. Each of these rights can be separately licensed under a variety of parameters and often with specific restrictions. Rights in a PAS can include:

- Term Limits. Instead of a perpetual license that is common for software development agreements, current trends are for limited terms with possible renewal options or subscription-style pricing.

- User licenses. Sometimes referred to as seat licenses, many software providers will limit the number of users that can access or process information. Access restrictions might allow limited access by members, employers, or other end users. Identifying the need for access by various stakeholders is a key factor and should be included in any RFP.
- Hosting v. Cloud. The current trend in PAS is for cloud-based solutions where system access, software, databases, and data are stored in remote data processing facilities (cloud-based). With any solution, it is important to understand the systems and clearly distinguish IP rights from data ownership. See “Privacy and Information Security” discussion below.

How do the fees pay for the software rights, access rights, and/or services?

All the rights discussed above should be addressed in the RFP for pricing comparison purposes. Current PAS agreements are often structured with separate fees for:

- Software licenses.
- User access fees.
- Customization v. configuration fees.
- Maintenance and support fees.

At contract negotiation, the crucial point is to understand exactly what the vendor is charging by avoiding legalese or industry jargon. Does the base PAS software license include all third-party license fees? Why are there user access fees if there is a license fee? What does customization mean (See Customization v.

Configuration below)? Will the vendor be performing specific functions related to member data? What is included in maintenance? All these questions should be asked and answered to ensure the parties are of accord and that the system is paying reasonable fees for the services it receives.

**Customization v. Configuration**

Imagine software as a customizable house where you can add on, remove, replace, and update. In the end, the basic elements of the house remain. The current software development environment is similarly customizable. We no longer need to plan for obsolescence or version 2.0, as software can be customized or reconfigured to meet specific design or architecture needs, or to take advantage of new technologies. This will also reflect the reality that change is a constant feature of retirement system administration, membership needs, laws, and regulations.

If the retirement system pays to customize the underlying

PAS software, who owns the new software? If the new software is inseparable from, and embedded in, the PAS, it is usually assigned to the vendor and included in the licensing fees. If the development is system-specific, that makes sense, however where the development is broader, say to incorporate other up and coming technologies, consider whether the retirement system should pay for that development. There can also be software modules (e.g., bridges, user interfaces, and templates) created by the vendor that are independently useful (i.e., post-termination transition) and should be owned by the retirement system.

The term configuration can mean different things to different parties. The vendor may use the term to



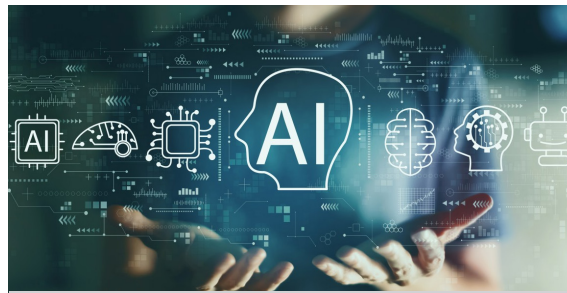
*At contract negotiation, the crucial point is to understand exactly what the vendor is charging by avoiding legalese or industry jargon.*

refer to customization of the software to accommodate a retirement system's operations. The retirement system may use the term to refer to day-to-day processing needs or input controls that should/could be accomplished by retirement system personnel. The former will likely be an additional fee to the retirement system, while the latter should not and should be addressed during implementation.

### Privacy and Information Security

The legal and statutory environment regarding data privacy and information security is in flux and varies according to jurisdiction. This lack of clarity is generally attributable to legislative activity or inactivity, but also the speed at which technology (e.g., cloud solutions, and AI) is outpacing both PAS development and regulation. Guidelines and best practices are constantly moving targets as technologies evolve making this a tough environment to create PAS and to implement and launch a PAS.

**Data Confidentiality.** Without exception, every retirement system has an obligation to maintain the confidentiality of member information and may have an obligation to maintain the confidentiality of other system information. An increasing, and alarming, trend is for the vendor to want ownership or unrestricted use of retirement system data after anonymization, aggregation, or de-identification (Aggregated Data). This provision, often buried somewhere in the licensing or services agreement, will allow the use of Aggregated Data by the vendor unrelated to the PAS or services to the system. Research has shown that there is a heavy risk of re-identification of Aggregated Data<sup>1</sup>, risking the confidentiality of the data.



*This lack of clarity is generally attributable to legislative activity or inactivity, but also the speed at which technology (e.g., cloud solutions, and AI) is outpacing both PAS development and regulation.*

**Data Storage and Processing.** Retirement system-specific limitations on where a PAS can store or process data (within the U.S., cloud v. on-premises, etc.) should be disclosed in an RFP and included in terms and conditions. This should include support and maintenance vendor locations, as many support call centers are in other countries and could require sharing data into jurisdictions with data privacy laws that could apply to your data.

**Information Security.** Increasingly, every PAS agreement includes detailed terms describing how the vendor will collect, transmit, process, store, distribute and delete information. While these terms regarding data processing, information security requirements, data security protocols and audits should meet legal requirements, they should also reflect your operational needs, which may require access to data by your third-party vendors.

### Contract Management

PAS agreements tend to be developed by the vendor to protect its rights and define the system without much consideration of the system's rights and needs. Additionally, the rights and obligations of the parties change as development makes way for implementation, which in turn makes way for support and maintenance. Multiple agreements are necessary and may be negotiated before the parties understand the impact of each phase.

**Implementation.** The most common point of failure is implementation. Best practices require that an agreement outline:

- Functional and technical specifications (not merely a statement of work).

- Development and payment milestones.
- Clear Change of Control procedures with named authorized representatives.
- Testing and acceptance criteria with timelines.
- Parallel test with 95%+ consistency with legacy system results prior to go-live.
- Off-ramp at any stage of development or testing if the vendor fails to achieve KPIs.

**Warranty.** Once a PAS has been implemented, the retirement system should have a complete warranty that will require the vendor to fix any issues within an abbreviated period. This warranty cannot be disclaimed or voided so long as the retirement system has not made (or allowed) changes to the PAS. Penalties for failure to fix warranty items can get creative ranging from total or partial refund to retention of a holdback percentage to extension of the warranty until identified issues are fixed.

**Termination and Data Extraction.** Termination issues to address include, but are not limited to, clarification of continuous access to the PAS, rights to extract its data into an accessible format or a successor vendor, clear notice requirements by both parties and escrow of software should the vendor become insolvent or cease functionality.

### Maintenance and Support

The structure of services for the maintenance and support of a PAS is specific to the PAS and the retirement system. Template services may be a good roadmap for the agreement negotiations but should

be tailored to the system’s needs.

**Services.** Once again, with multiple agreements, it is imperative to consider whether the retirement system is already paying for certain services as part of the license or user access fee. For example, if the vendor is charging to update the system on a regular basis, is that part of the license fee for the PAS to perform according to the specifications? There can also be fees for other work, such as imaging of documents, that is being performed by retirement system personnel.

### Service Level Agreement (SLA).

The SLA might be an exhibit to the PAS agreement (which should continue when the PAS implementation has been completed) or a Maintenance and Support (M-S) agreement. However, a retirement system should understand how downtime for certain functionality could affect operations. Any SLA should ensure that critical functions have short response

and service escalation times, while less critical issues are reasonably considered.

How each retirement system gets to Go-Live for a new PAS is a journey of practicality. It’s also important to recognize that the journey requires a great deal of internal and external assessment of business processes, technical and operational requirements, and contractual alignment from the issuance of the RFP to implementation and beyond.

*Thomas Dover and Michelle Mellon-Werch are both Partners at Nossaman.*



*Once a PAS has been implemented, the retirement system should have a complete warranty that will require the vendor to fix any issues within an abbreviated period.*

### Endnotes

<sup>1</sup> Nature Communications, 23 July 2019 (article 3069), nature.com/articles/s41467-019-10933-3.