Retirement Research Center
A DCIIA ORGANIZATION

SPARK INSTITUTE
SHAPING AMERICA'S RETIREMENT

SPARK Study: Understanding Data Privacy Sensitivities Across the Defined Contribution Industry

April 2023

INTRODUCTION

As plans have evolved since the early days of ERISA, defined contribution (DC) plans have largely replaced defined benefit plans as the primary retirement savings vehicle. As a consequence of this, plan participants have increasingly needed help with their retirement savings plan decisions. Moreover, the DC plan has also become the nexus for financial matters beyond the retirement plan, often referred to as Financial Wellness support. Actionable guidance can require personal data about and/or from participants. Indeed, ready access to data is a central component to many of the most promising opportunities for progress in the DC system, and these needs will grow as topics such as decumulation become a larger focus. Data privacy and data sharing are critical to all parts of the DC ecosystem.

In April 2022, SPARK and DCIIA hosted an Industry Workshop on Privacy and Data Sharing. Over 60 senior industry leaders attended this in person, and 35 participated virtually. This group explored data needs, regulatory concerns, and diverse practitioner viewpoints. There was recognition of the increasing need to support DC plan participants, and the critical role that data plays, however, many within the industry had differing perspectives.

Subsequently, SPARK engaged the DCIIA Retirement Research Center (RRC) to conduct this exploratory study, focused on qualitative research across the key constituencies in the DC ecosystem. The goal of the study, detailed here, is to improve understanding of participants', plan sponsors', recordkeepers', and advisors' perspectives regarding data sharing and data privacy—where they align, and where they differ. Over the course of May to October 2022, the RRC facilitated interviews and focus groups amongst these constituencies.

Note: In this study, data sharing refers to plan fiduciaries providing access to data for the purposes of servicing employees. In contrast, data privacy pertains to security measures and internal operations with the objective of encrypting and safeguarding participant data. The latter was not the direct focus of this study; however, it was part of the discussions.

KEY FINDINGS

PARTICIPANTS

Four participant focus groups of around six individuals were conducted across different generational cohorts consisting of younger males, younger females, older males, and older females. The main takeaways included:

- Participants are often seeking support from their employers.
- They are willing to share their personal data with increased transparency on usage and more control on third-party sharing.
- Trust stems from brand strength.
- Willingness to share data for a clear purpose if they see the value.
- Desire limited distribution of "added" details, akin to lending; needs to be clear, defined, and restricted.
- Trust is key—employees largely trusted their employers with data usage; however, concern grew when sharing data for purposes outside of direct employee benefits. This may have implications in employers' ability to serve as the conduit for financial wellness services.

PLAN SPONSORS

In total, fourteen plan sponsors were questioned through interviews or focus groups, including a mix of small-, medium- and large plans. Additionally, an online survey was deployed, with 83 plan sponsors responding. The main takeaways included:

- The topic of data privacy and data sharing has been an increasing focus. Many have formalized policies and procedures, including limiting data access/sharing, reviewing contracts, etc.
- Current consensus view is that data is ultimately owned by the participant; however, the plan sponsor manages and protects it (not the employer).
- The bulk believe data is a plan asset—this held true, even when pressed on what that may imply under ERISA. However, most do not fully understand these implications.
- There are times when data needs to be shared and there are times when data needs to be accessed. When data is shared, it is sent and under the control of the recipient. Data shared is akin to lending—it is not given to the recipients but can be accessed in a limited manner and should terminate when that relationship ends.
- For smaller plans, the distinction between the employer and plan sponsor is less clear.
- Financial wellness products are viewed as separate, as the employee opts in, which creates an agreement on the use of data outside of the plan/employer. Data usage and restrictions are then imposed by the employee rather than the plan/employer.
- Some concern, among small- and mid-sized plans, around usage of participant data within the recordkeeper relationship.
- Employers are concerned about expanding services, given the litigious environment.
- Lack of clarity and guidance is challenging. Many employers believe they would benefit from clear, specific guidance from the DOL to create industry standards and a safe harbor for plan sponsors.

RECORDKEEPERS

In total, individual interviews were conducted with six major recordkeepers. The representatives usually included two individuals per organization, representing DC leaders, legal, privacy, and/or data/security professionals. The main takeaways included:

- Ultimately, they believe the participant owns their own data, but the plan sponsor/employer has an obligation to control and protect that data.
- Because the recordkeeping contract is with the employer, it is generally felt that the employer controls participant data (not the plan sponsor).
- Acknowledge nuances of data elements, and varying sources of data.
- Recordkeepers believe they play more of a custodial role. However, this does not absolve them of risk.
- Report that they rely strictly on plan sponsor/employer direction for data sharing/access.
- Indicate increased scrutiny and risk around housing/sharing data, including both internally and externally.
- Concern with regulatory uncertainty as complexity is increasing with participant services, and the influence of state regulation – "50 rogue states."
- Lack of standardization makes fulfilling advisor requests for access extremely challenging.
- Sentiment that Washington could provide more clarity, although concerned that it could lead to complexity and/or ambiguity (i.e., be careful what you wish/ask for…).

ADVISORS AND INDUSTRY PROVIDERS

The DCIIA RRC conducted six interviews across six firms, including one- to two individuals from four of the major RPA Aggregators. The main takeaways included:

- Needs for data vary by advisory firm.
- Most don't differentiate between role of plan sponsors and employers; view as synonymous.
- Permission is typically granted through employer/plan sponsors (recordkeeper is merely the conduit).
- Recordkeepers are not providing data, unless instructed to do so. Advisors report often getting pushback even after instruction from plan sponsor is provided.
- View lack of access to data and connectivity as hurting participants.
- Implicit and explicit costs to the recordkeeper are a deterrent. Recordkeepers are also a competitor for advisory services.
- Lack of standardization makes the process more challenging.

MAIN THEMES AND IMPLICATIONS

1) Increasing awareness and priority

The topic of data privacy and data sharing has been an increasing focus for all parts of (and parties in) the DC system. This has resulted in more formalized policies and procedures around data sharing and data security, and notably more friction around, and resistance to, data sharing.

- Employer concern resides around cybersecurity, data privacy, and litigation. Employers have spent more time on processes and contracts, ensuring data usage and, where applicable, prompting limits. However, to date, this has been more of a focus among large plan sponsors than small- or mid-sized employers.
- Recordkeepers have implemented more stringent guidelines for sharing data internally and externally. This has ramped up given litigation and recent state (e.g., California) regulations. Internal hurdles and intra-organization sharing have also been curtailed. Data sharing hurdles have risen, and require a clear purpose and benefit, and a critical business need. To a lesser extent, this also extends to sharing non-PII data, but there remains a cost/benefit focus that may be limiting progress and innovation.

2) Data "grey" zone

Foundationally, the question of data access, control, and ownership begins around defining the data elements. The distinction is not always clear, and sources of data become blurred with the possible inclusion of payroll, the plan, recordkeeper, employer, etc. This becomes more extended if there are additional connections with/through a financial wellness provider. This discussion becomes increasingly complex once nuances such as terminated workers enter the equation.

Further, there are distinctions between housing the data and accessing or utilizing that data. The usage of data defines the value of it. This was a distinction when using or sharing data - parties need to understand how it will be used and the benefit that it would provide, and to/for whom.

3) It's about control, not ownership

Almost all the parties we surveyed or interviewed agree that the participant owns their own personal data. Certainly, the plan participant believes this. However, within the DC system, all constituencies acknowledge the distinction between ownership and access/control, and the need for the plan to be managed holistically (i.e., not requiring employee permission to do nondiscrimination testing). Participants are not able to remove their data, personal or collectively gathered, from mandatory plan obligations, such as nondiscrimination testing or plan performance reviews. Employers agreed that participants cannot selectively remove their permissions for what is considered to be custodial obligations; data protection applies to activities and services outside of normal plan operations.

Ultimately, the constituencies we spoke with generally agree – either the employer or the plan sponsor have a responsibility to protect and control that data. That is, people generally agree that the employer/plan sponsor has some (implicit) contractual responsibility to safeguard the data but does not own the data itself. They merely control access to, and use of, the data. In addition, all constituencies view the recordkeepers as a custodian that houses and protects that data.

4) Plan sponsors believe the plan controls the data

Although courts have consistently ruled that data is not a plan asset under ERISA, the bulk of plan sponsors currently believe that the plan should control access to and use of data. When asked specifically, they also express the bias that data is a plan asset under ERISA. This held true, even when pressed on what that implies and possible fiduciary implications. However, it seems likely that most do not fully understand the nuances and broad implications of this perspective (as the DOL indicated, "If data is a plan asset, it would need to be held as an asset of the trust, meaning the trustee would always need to be in control of the data. It cannot be in the possession of anyone but the plan trustee"). That said, larger plans are more aware, yet still generally held to the notion of data being a plan asset. When asked to select one (employer, plan, or employee, nearly two-thirds (62%) of plan sponsors surveyed indicate that the plan is ultimately responsible for data.

It is notable that recordkeepers have a different view and generally believe the data is controlled by the employer. This is, at least in part, because their contracts usually reside with the employer, not the plan.

5) Access to data is contractual

Across all parties, access to data is based on contracts residing with the employer/plan sponsor and/or the participant.

Notably, recordkeepers all indicate their role is contractually defined and custodial in nature. However, this does not obviate their risk and need to safeguard that data. They are simply relying on the employer for direction.

Similarly, recordkeepers feel that advisors or financial wellness tool providers would also need contractual relationships with the employer/plan sponsor. Advisor needs vary by organization, but typically agreed that permission should/would be granted through the plan sponsor. That said, concerns remain regarding how any data sharing would be executed, including the lack of support from the recordkeeper given the growing number of hurdles and lack of uniformity.

All agree that participants providing additional information (whether to the plan, the recordkeeper, the advisor, or some other third-party provider) would also clearly be subject to contractual limitations; however, much uncertainty exists on how to deal with and operationalize this.

6) Limitations: "lending" with an on/off button

Employers and employees both believe data is "loaned" for the purposes of plan administration rather than being given away. Under this view, the access to the data remains in place while the relationship is in place and terminates when it is ended.

This desire for control exists from employers and participants. For example, participants generally report a willingness to share data (for financial wellness tools, for example) when they see the value and have the ability to control the usage. This requires transparency and a partnership with workers.

7) Financial wellness solutions: a third layer

The DC plan is increasingly seen as a nexus for financial wellness, and adoption of new tools and features will continue. As employees grapple with how to spend their "next best dollar," support and guidance will need to be provided. This, of course, is often driven by data; employee adoption will be driven by trust. However, they prefer the employer to be a conduit, vetting a third-party provider. Participants do not want their employer to have access to their broad financial information.

Employers often view financial wellness solutions as a separate, add-on feature, that employees can opt into. There are concerns around these new additions and new relationships.

Recordkeepers see these solutions as continuing to grow through strategic partnerships. The data questions/challenges raised are viewed as significant barriers to innovation and progress. This is due to these services being viewed as creating separate relationships between the third party and the plan, and then ultimately, the participant.

8) Challenges: risk, regulatory uncertainty, and lack of framework and standardization

Litigation and regulatory risk are top of mind with employers and recordkeepers.

Many employers believe they would benefit from clear, specific guidance from the DOL to create industry standards and a safe harbor for plan sponsors. It was noted they want guidance with flexibility, and not seeking increased burdens or over-regulation.

Recordkeepers and advisors also believe guidance could help. However, they also noted it could be a double-edged sword. Many recordkeepers indicated the added complexity of state regulations.

Advisor and recordkeeper relationships remain complex. There are multiple challenges here, both concerning operational complexity and competitive costs. Business models are converging, and different segments are increasingly becoming both partners and competitors. Recordkeepers indicate they will share data/send information at the behest of the employer only. However, even if the plan approves, there are also processes in place to understand the implementation cost and risk. The lack of standardization, and frequency of demands for data from many in the industry, create a challenge.

9) Looking ahead: amenable to broader solution

A third party, consistent, and common platform (data housing/consortium) would be a significant benefit for the entire DC ecosystem. After moving past natural operational hurdles and questions, all DC stakeholders indicated this would be beneficial for the industry and their organizational practices.

Standardization of data requests including formats, layouts, and data elements that would be operationally beneficial. Further, the mechanism to share information is needed, and standardization for collection, storing, sharing, and disposing of data elements.

The pipeline to connect data and organizations would allow for things to (eventually) be more seamless, secure, cost effective, and ultimately benefit the participant. Many indicate the barriers of forming the consortium model are not technology-based, rather organizational that would require time, effort, and an advocate.

NEXT STEPS

Phase Two Research Study

Building on the work of Phase one of this study, additional exploration is needed to more fully understand the depth of drivers and clarity of the current state. This includes testing future solutions, evaluating feasibility of future options uncovered, including perceptions and obstacles. Ultimately, determining a strategic path forward based upon an evaluation across constituencies.

Phase two will include a deeper dive across the DC system, encompassing:

- Broad quantitative analysis
- Strategic supplemental qualitative analysis
- Ideation with industry and policy thought leaders

Specifically, implementation across entities will include:

- Participants: Online blind survey of 2,000 workers, nationally representative
- Plan sponsors: Larger, more in-depth survey of 150 employers, with varying size and segmentation. Additional follow-up interviews and focus groups to supplement and explore nuances.
- Advisors and Recordkeepers: Follow-up interviews across organizations, targeted by topic.
- Industry: Interviews and additional perspective obtained from others in the DC system.

SPARK/DCIIA Data Summit in Washington, DC

Following this analysis, a second Data Summit would be recommended connected to the DCIIA/SPARK Public Policy Forum (June 6th-7th) in Washington, DC. This convening can facilitate deeper exploration into the study findings, as well as obtain perspectives around future focus. Topics for the Summit can include:

- Report on implications of phase 1 (and possibly phase 2) of the research
- Explore opportunities/challenges presented by AI/ Blockchain and other emerging tech
- Facilitate panels with key constituencies on next steps and the path(s) forward

Explore Feasibility of a Data Consortium

Building on the work of Phase one of this study, additional exploration on the feasibility of the Data Consortium is needed. This can be accomplished with a smaller working group, alongside the Data Summit in Washington, DC. Further Phase two of the study can also explore reactions and perspectives related to this concept.

IN-DEPTH STUDY FINDINGS

PARTICIPANTS

Four participant focus groups were conducted across different generational cohorts consisting of younger males (21-35 years of age), younger females (21-35 years of age), older males (45-55 years of age), and older females (45-55 years of age). All participants reported they are actively contributing to a defined contribution plan and are the primary or joint decision-maker on finances in their household.

Participants shared their prior experiences with data sharing behavior personally, and their behavior on platforms such as social media. Further, they were probed on data privacy in the context of employer financial wellness programs and employer-sponsored guidance. Specifically, the trade-off between more accurate and useful guidance versus complete data privacy was queried. Finally, trust was discussed, around their employer and other parties in the DC system.

METHODOLOGY

The DCIIA RRC conducted four focus groups with about six individuals in each group. The 90-minute focus groups were conducted by Warren Cormier in August 2022 through a virtual platform. Interviewees were promised anonymity and are not identified in this report.

Respondents were screened and selected to include a diverse group of workers using the following criteria:

- Gender (almost half were women)
- Age range: 21-55 years old (separated by generational cohorts in focus groups)
- Actively contributing to a 401(k) plan
- Household income ranging from $25,000 and more annually
- Individuals working at government agencies, advertising firms, life insurance firms, and financial service firms were omitted
- Diversity across race, geographic locations, and occupations

Technical Note: Qualitative research is helpful in developing hypotheses surrounding a topic. However, because of the small sample size, the results described should be viewed as directional and in need of quantitative confirmation. This report is preparatory for a more in-depth study.

DETAILED FINDINGS

Existing Data Sharing Behavior

Participants were questioned on their existing data sharing behavior across normal, daily life as well as within financial wellness situations. Most participants are active on social media and online shopping websites requiring consumer data. When probed on their levels of trust in these websites regarding data usage, two key themes emerged:

1. Participant trust is established and built through regular contact (communicatory consistency) and overall operational efficiency with participant-facing services.

2. Participants did not distrust companies themselves, but data privacy concerns were centered around security breaches once companies continued to share data to third parties, following initial authorizations for use.

Many participants express trust in online retailers such as Amazon, Etsy, and other large companies due to the size of the firm and industry rapport. Although they acknowledge their data is being used regularly by these organizations for other purposes, most did not express concern. Most view this sharing as a “cost of doing business” mentality, around convenience. However, participants have relatively more distrust in smaller organizations and, notably, independent individuals or service providers. With data breaches as a high concern, participants believe smaller companies or practitioners lacked robust tools or interest in protecting sensitive consumer information. In addition, name brand recognition is a significant influence in building trust.

Comparing across generations, younger workers believe data sharing is a necessary risk due to the fundamental need for user data for business purposes. However, older workers and pre-retirees are more hesitant to provide sensitive information due to a lack of control and transparency once data is initially provided. Older workers and pre-retirees express concern that their data would continue to be used beyond the original purpose to unknown third parties. Regarding aggregated, deidentified data, older cohorts are more confident that data collected could be anonymous, however, younger generations express disbelief that data usage would ever be fully anonymous and excluded from business marketing purposes.

Regarding personal information that is shared, most participants indicate their preferences for:

1. **Transparency**
   They want to be fully aware of how their data is being used.

2. **Control around use and collection**
   Participants want to have a level of control as to where and how their data is being used, and they want to manage how it is gathered.

Interestingly, older women are more likely to be risk-averse and less likely to share data or personal information (PII) provided, including birthdays, income, and marital status. Male participants, in contrast, align with younger cohorts in the belief that sharing personal information and data is an inevitable requirement.

> *"I do actually feel strongly about providing my real birthday on these sites from a privacy perspective."*

> *"I trust [large retailers] more than my employer with my data privacy."*

Financial Wellness Data Preferences

Participants were asked a series of questions exploring their data sharing practices related to employer offerings and financial wellness programs. Financial wellness services mentioned included emergency savings, student loan repayment, retirement planning, and debt management, amongst others.

Participants are generally supportive of the trade-off of potential data security for more personalized, accurate program offerings. However, there are data security and privacy concerns by some which reflected the continued need for transparency on data usage. Most participant's employers offer one or more wellness services, and participants believe they are a helpful resource.

When probed on the personal struggles with determining where to spend their 'next best dollar,' younger female participants believe that debt should be paid down as a higher priority before addressing emergency savings and other recurring payments. Younger females (women vs women, men vs men) are more receptive to engaging with financial wellness services to help guide their decision-making.

Conversely, younger men express distrust with sharing additional financial or personal information due to the belief that they could manage their household's finances independently without the need for external support or dedicated programs.

> *"I mean if you're asking 401(k) stuff, then yes, I do take advantage of that. If it is more of 'let me help you make a monthly budget,' I don't take advantage of that. I do things on my own end, so it depends on what benefit they're offering financially."*

Younger men list self-directed products such as Mint and other mobile-based applications as their primary tools for managing household expenses and savings. In general, younger men believe projections and variable-based modeling require too much personal information for the overall value provided.

Both younger and older male participants would like increased regulation on data usage and sharing due to skepticism on value-adds from wellness programs and guidance alongside distrust of potential government involvement.

> *"What you give permission for and what actually happens might be two different things. I do think there is somewhat of a distrust, for good reason, with government regulating things."*

All participants (male and female) collectively agree that larger companies and employers are more trustworthy than independent practitioners or smaller firms due to perceived differences in company-wide priorities on data privacy. The channels participants noted that are safe for sharing information included usage of emails and shared files through encrypted upload portals. There was a unique sentiment, notably with younger men, that employers should be trusted and there was a willingness to trust. Notably, some participants indicated that employers who are more transparent and trustworthy with sensitive participant data are more attractive for employment purposes.

However, trust in employer data management stalls around data warehousing, and increased need for specifics, including marital status, demographics, locations, and previous employer financials. Younger and older men prefer maintaining primary control of data access to selectively provide specific personal information as needed.

Limiting Employer Data Sharing

Perspectives around the employers' role in sharing data to third parties, particularly for financial wellness services, are mixed. Many preferred the employer to make information easily accessible and available for participants to control sharing; however, they do not want the employer to have access to their financial details outside of the retirement plan.

Some female participants believed that employers should not utilize data sharing capabilities on their behalf, and rather that it is the participant's job to establish that connection with outside service providers.

> *"I would not give permission. To be honest with you, I would want to give the information to the advisor directly to be more comfortable. I don't think it's necessarily the place of my employer to establish that relationship unless they were just setting up the initial contact with the advisor."*

> *"I am not ok sharing that information with my employer, I do not think it's their business. Call me a cynic, but I do not want my employer knowing what my savings, 401(k) balance, or assets are."*

Several male participants are comfortable with their employer sharing personal information with external advisors or service providers, but only if they are involved with general supervision over the process themselves. This follows the consensus that participants value their own control and ownership of personal data and have limited trust of their employer to access or share this information to third parties.

In addition, nearly all participants have concerns regarding employer access to outside financial information and 401(k)s. There is a clear distinction between participants willingness to engage in current wellness offerings, however, participants are resistant to allow their current employers' access to extra information given participants' willingness to provide personal information for data purposes was conditional. With broad resistance to allowing employer access to 401(k)s and previous financials, there are hurdles to comprehensive utilization of wellness programs.

Furthermore, participants express interest in maintaining primary control of usage of their data. Most participants are hesitant to share data based on a 'chain-reaction' possibility of employers sharing data externally after initial permission.

Uncomfortable with sharing control to other service providers, programs, or employers, some female participants were concerned that if they granted permission for one program, the permission would be extended for other business purposes without their explicit knowledge. Due to this 'chain reaction' concern, they strongly prefer retaining primary control of their data.

> *"If I'm giving them permission for that [sharing financial wellness information], then I don't know what else I'm giving them permission for. If they [advisors] want certain things, I can get it for them by myself."*

Participants responded positively when asked about having their accounts and information consolidated to make handling their finances simpler and provide a more helpful platform. The majority were comfortable with sharing information for this purpose; however, the question remains by whom.

Participants said they would be comfortable entering their information into a secure portal if it gave them a broader and more accurate overview of their finances. Additionally, they felt positive about outside programs even if it required more personalized data to be shared. As long as they did not have to provide login/access to their accounts, respondents agreed that more personalized support and guidance would be useful.

> *"I would be the keeper [of the information]. I would get it myself and forward it to them. Even if the information changes month-to-month, I would rather be getting them that information rather than giving access to my account."*

> *"I am happy to provide a full picture of my account and periodic updates as needed but would not be comfortable giving them access to any of my accounts."*

PLAN SPONSORS

Three plan sponsor focus groups and three specialized interviews were conducted across differing plan sizes, including Small (<$50M), Medium (<$250M), and Large (>$1B+) plans. In total, fourteen plan sponsors were interviewed, of which two represented public sector plans. All are involved in benefits decision-making within their organizations. In these focus groups, plan sponsors discussed current utilization of their plan's information, perspectives around ownership/control of plan data, implications of regulatory environment, and current practices with vendor access and usage.

In addition, a brief survey was deployed across the DCIIA Plan Sponsor Institute (PSI) to gain insights into the current concerns of plan sponsors relating to service provider data sharing, perspectives on primary data control and access, as well as the intersection of financial wellness services.

METHODOLOGY

The DCIIA RRC sought plan sponsor perspectives through focus groups and a targeted online employer survey.

Focus Groups

The DCIIA RRC conducted three focus groups with four to five individuals in each group. The 60-minute focus groups were conducted by Warren Cormier and Pamela Hess in September and October 2022 through a virtual platform. Focus groups were comprised solely of private organizations. Further, three additional one-on-one interviews were conducted with plan sponsors, two from public plans, and one a large private plan. All interviewees were promised anonymity and are not identified in this report.

Plan sponsors were screened and selected using the following criteria:

- Plan assets spanning small to large plans (plans of $8M to well over $10B)
- Active benefits/DC plan decision-makers within their firms
- Organizational diversity across industries such as healthcare, financial services, higher education, retail, and more

The focus group discussions probed a variety of areas, including:

- Perceived ownership and control of retirement savings DC plan data
- Current usage of DC plan data
- Data access controls in place, and concerns around data
- Perceived risk, consequences, and rewards around data sharing
- Data implications surrounding financial wellness services and tools
- Perspectives around current and possible future framework as well as regulatory guidance

Technical Note: Qualitative research is helpful in developing hypotheses surrounding a topic. However, because of the small sample size, the results described should be viewed as directional and in need of quantitative confirmation on a larger scale than the additional survey. This report is preparatory for a more in-depth study

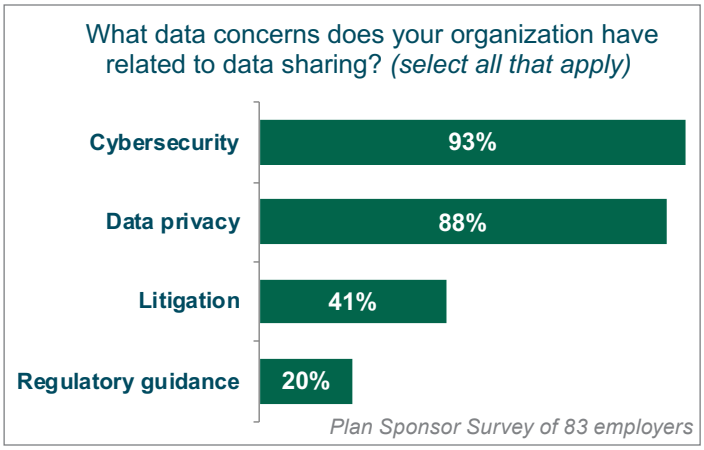
Online Survey

Additionally, an online employer survey was conducted with the DCIIA Plan Sponsor Institute (PSI) members. In total, 83 responses were received. Three-quarters of respondents report plan assets sizes over $1B in value, and over 10,000 participants. Organizational industries widely varied across financial services, manufacturing, healthcare, technology, and more. The types of DC plans represented included 401(k) (71%), 457 (12%), 403(b) (7%), and 401(a) (5%).

DETAILED FINDINGS

All plan sponsors report an increase in time and attention to data privacy and data sharing issues within their organization during the past 18 months. This was also true across 100% of focus group participants.

The main areas of reported concerns regarding data privacy and data sharing concern varied. The online survey revealed a key focus on cybersecurity and data privacy, followed by litigation and confusing/lack of regulatory guidance. This is consistent with focus group responses, although there is some variance by plan size. Litigation and security are a greater concern amongst larger plans.



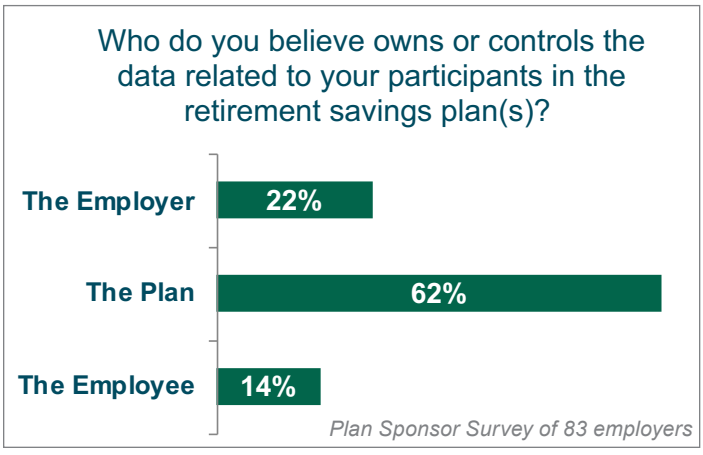
The efforts to maintain secure data privacy and limited access control are robust with 89% of plan sponsors regularly reviewing their cybersecurity protocols to ensure adequate measures. Many plan sponsors have only recently begun to establish internal policies and procedures for data sharing and access, while a significant number have limited their reviews to annual audits. Focus group interviewees noted recent development of privacy controls outside of internal and external file sharing, where access to PII and aggregated data is solely limited to plan trustees and fiduciaries.

Additionally, plan sponsors have spent more time and attention on increasing organization of documents to ensure regular reviews of service provider agreements. These agreements can detail operational processes, cybersecurity-related concerns, and, most importantly, contractual limitations on data access. Due to changing regulations and new benefit offerings, plan sponsors agree that service provider agreements need to be regularly reviewed and updated, outside of renewals and onboarding processes, however many plans have not taken active steps to accomplish this.

Data Control

Plan sponsors discussed the concept of "ownership" and control of participant data and were asked which entity holds primary responsibility for participant data, ranging across the employee, the employer, or the plan (where data would be considered a plan asset). Nearly all acknowledge that it is ultimately the participants' data. Across the focus groups and plan sponsor survey, the majority of respondents believed that the plan has primary control of participant data due to a perceived sense of their fiduciary responsibility.

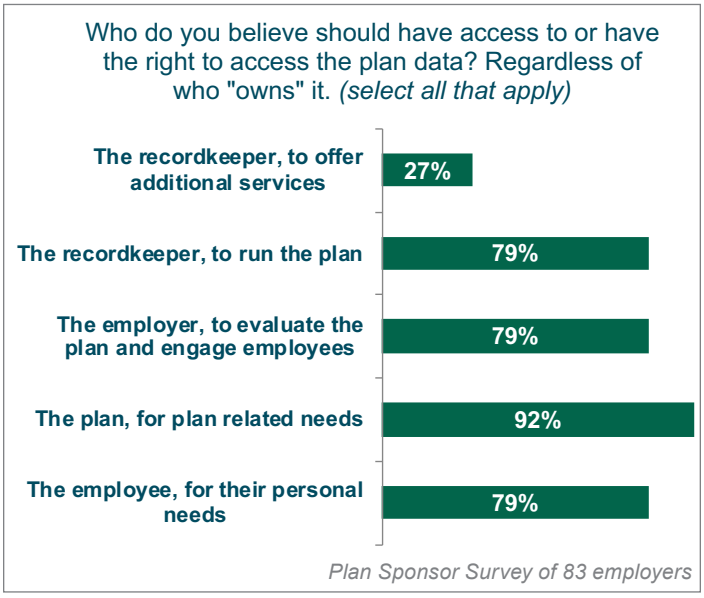
> *"Participants own their own data. We are ultimately responsible for protecting that data."*



Within the plan sponsor survey, 62% of respondents name "the plan" as holding primary control while an additional 22% of respondents indicate "the employer" holds control. Notably, only 14% of plan sponsors believe participants maintain primary control of their data, as opposed to nearly all participants, in the focus groups, believing they held primary ownership.

When probing this concept in focus groups, interviewees across all plan sizes believed that "the plan" controlled participant data which also implicated ERISA duties. Even when the group was probed on the potential implications of this, the belief was steadfast. Notably, most do not fully understand the broad effects of a possible "plan asset" status.

Plan sponsors believe fiduciary responsibility extends to continuously managing participant data privacy and controlling access to both personal identifiable information (PII) and aggregated information, partly due to ERISA obligations applying during the original collection of participant data.



Larger plan sponsors, in recognition to participant data concerns and increased litigation, have begun to implement the approach of 'less is more' around data sharing. In general, plan sponsors require limited participant data sharing for full integration into basic retirement plans, however, more information is required when extending additional financial wellness services and benefits from recordkeepers, financial advisors, and other third-party administrators. Plan sponsors, aligning with current industry trends, have encountered complications due to increasing interest in providing additional wellness services, however, litigation concerns and some distrust in recordkeeper usage of data beyond the scope of normal needs have impacted decision-making. Smaller plans were less likely to be as hesitant and more likely to work with FINTECH providers.

Current litigation trends were commonplace amongst discussions across all focus groups, where plan sponsors expressed concerns in potential lawsuits related to cybersecurity. Despite recent legal rulings that plan data is not a plan asset, plan sponsors anecdotally believed ERISA fiduciary duties would be implied within potential cases. Focus group participants sought to differentiate between data sharing, an action set into motion by the plan sponsor, versus data access which focused on financial advisor and other third-parties. Plan sponsors, as a result, raised multiple concerns related to their recordkeeper relationships alongside developing contractual practices on data access to help mitigate potential litigation.

Relationship with Recordkeepers

Regarding data privacy measures, plan sponsors indicate a broad and extensive view of data privacy, where the concept of 'standing authorizations' for data usage was limited, even amongst recordkeeper activities. Plan sponsors do not believe that recordkeepers hold primary control of participant data, rather they believe that recordkeepers have a shared responsibility of maintaining high data privacy measures. By recordkeepers currently having separate regulatory requirements in the management of participant records, and sharing in cybersecurity responsibility, plan sponsors were confident in the belief that recordkeepers did seek to protect participant data. Two key findings emerged regarding plan sponsor relationships with their recordkeepers:

1. Plan sponsors were concerned with potential 'unintended consequences' of recordkeepers using data for product development and ancillary sales.

2. Recordkeepers did not have 'standing authorizations' to use or share data outside the scope of original functional agreements, such as with offerings related to emergency savings, rollovers, advice, and other related services.

Plan sponsors have diverse perspectives and policies with their respective recordkeepers. Larger plan sponsors generally have contractual agreements with specific limitations on data needed for administrative needs. Recordkeepers were not permitted to cross-sell data, while separate data security rider documents are also common. Plan sponsors regularly ensure these agreements are being upheld with some opting to randomly contact participants and check communications to ensure compliance. Most plan sponsors believe cooperative agreements with vendors are required to avoid 'unintended consequences' of recordkeepers utilizing plan data for other purposes. This hesitancy is further demonstrated with 57% of plan sponsors reporting a level of concern on service providers utilizing employee data to market products unrelated to their retirement plans. This is particularly pronounced with smaller plans. However, it is also notable that smaller plans are less likely to curtail or manage recordkeeper access to their plan participants.

Nearly eight in ten plan sponsors agreed that recordkeepers required access to plan data in order to 'run the plan,' however, only 27% agreed that recordkeepers required access to offer additional financial services.

Plan Usage of Participant Data

Employers of all sizes utilize aggregated plan data to explore the efficacy of the plan and identify potential shortcomings in benefit offerings. These reviews are to ensure value and quality of the plan and ultimately to improve participant outcomes and understand feasibility and the need for plan design changes. Often, plan sponsors believed reviewing plan data was required to fulfill their fiduciary duties in respect to plan performance and longevity.

Large and medium plan sponsors, in particular, used plan data to support workforce planning initiatives in collaboration with Human Resources (HR) and senior executives.

> *"If 75% of them are eligible to retire [referring to critical internal work group], then there needs to be some strategic planning around that at a very high level."*

The use of plan data, even at the aggregated level, raised concerns about who had the ability to request and access the information. When probing on who has access to plan data, most plan sponsors agreed that trustees or a governing body had unrestricted access to aggregated data. However, larger plans believed a smaller subset had access to individual data where requests for information were limited to ad-hoc decision-making.

> *"The ethical line can be blurred very easily when that question is being asked."*

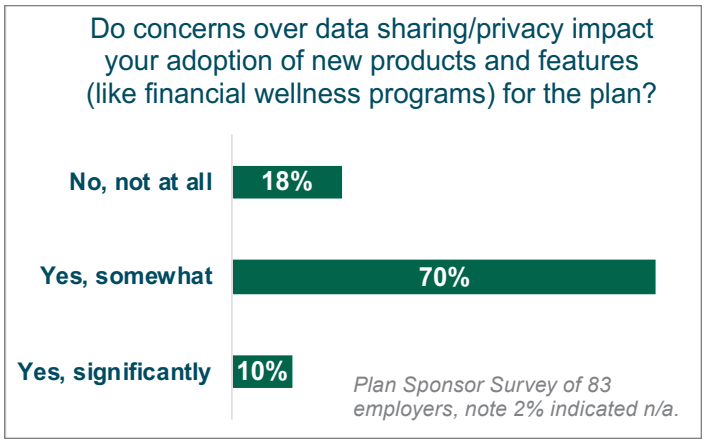
Further, across smaller plans, the line between the employer and the plan sponsor is less clear. Given the smaller team and resources, these workers wear multiple "hats" and often act as the decision makers for plans alongside the primary support for employer budget planning, operational management, and sourcing and implementing additional financial wellness services. These smaller teams usually have less formal, written protocol and limited centralization on access to plan data.

Financial Wellness Tools

As the DC plan becomes a nexus for financial wellness, its scope has expanded beyond traditional retirement savings. While student loan debt and emergency savings tools are currently offered by 33% and 40% of plans surveyed, respectively, many more are planning to add more tools in the coming 18 months. This is additive to many that currently offer budgeting/debt management, financial planning, and healthcare/HSA planning tools.

There are concerns around losing control, where the employee has selected a service outside of the plan. Those agreements, or connections, are viewed as separate and at the behest of the employee. Therefore, it is viewed separately, but those lines continue to blur.

> *"We're ultimately responsible to protect the data. Now there are all these add-on services to help with things like planning, financial wellness, wealth management, emergency savings accounts. As this continues, at what point do we start losing control."*



These hesitations on data access and utilization were also found with respect to allowing financial advisors or further external administrators access. Focusing on financial advisors, plan sponsors of all sizes generally had more concerns on advisor's data security practices and warehousing protocol.

When probed on the scenario of whether plan sponsors would allow participants to share login credentials or general plan information with financial advisors, the majority of plan sponsors denied access or requests. Notably, smaller plan sponsors did indicate approval through a written agreement releasing fiduciary duties related to information protection, but all other plan sizes had standard denial of such requests.

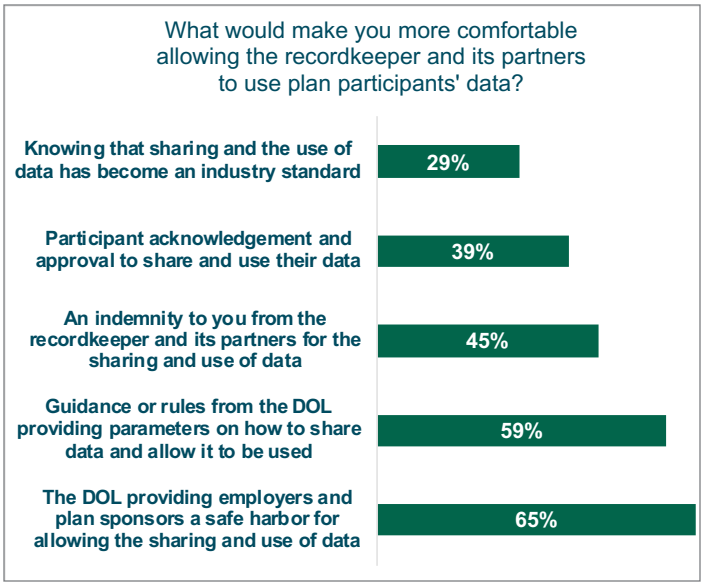
The DCIIA RRC further explored these alternative options to gain more insights into data sharing protocol across the Fintech space. Plan sponsors discussed tools, similar to PersonalCapital, which leverage Application Programming Interfaces (APIs) to allow for high-level oversight of balances and plan information as opposed to allowing user access to process transactions. In addition, participants can revoke consent with full removal of data at any time, allowing for more simplified onboarding and user termination procedures.

Finally, several plan sponsors mentioned challenges when changing service providers or recordkeepers, within the financial wellness space. That data does not necessarily migrate with the plan/participant. Several employers indicated a loss of data that was substantial and problematic.

Risk and Regulatory Guidance

Plan sponsors of all sizes have expressed concern around risk, and lack of guidance or standards in the industry.

> *"Data is everyone's responsibility; we can't do it all as the plan sponsor."*



Notably, when asked, "what would make you more comfortable allowing the recordkeeper and its partners use of plan participants' data," the majority of plan sponsors requested more DOL guidance. Within focus groups, plan sponsors of all sizes provided further detail into this shared sentiment to indicate a need for clear, specific DOL guidance to provide either an industry standard on data practices or a safe harbor to reduce the potential for litigation.

Plan sponsors also agreed that all service providers handling plan data should be held to a standard, basic level of fiduciary responsibility in ensuring secure access and sharing practices. However, smaller plan sponsors indicated their agreement under the belief that general cybersecurity should be everyone's responsibility, whereas larger plan sponsors believed current DOL guidance does not appropriately address all perspectives and could complicate things. Many wanted guidance with flexibility. There was caution around increased burdens and potential overregulation.

Plan sponsors were asked about their interest in standardization more broadly in the industry or more specifics from future DOL guidelines. The majority showed interest in standardization of data requests and usage by all third parties (such as recordkeepers, financial advisors, institutional advisors).

RECORDKEEPERS

In total, six individual interviews were conducted among the major recordkeepers. The representatives usually included two individuals per organization, representing DC leaders, legal, privacy, and/or data/security professionals.

In these interviews, recordkeepers discussed their perspectives around data privacy/sharing, operational procedures related to data access, relationships with advisors and consultants, and interest in an industry-wide data standardization/platform.

METHODOLOGY

The DCIIA RRC conducted six interviews across recordkeepers alongside interviews with six advisors. The 45- to 60-minute interviews were conducted by Warren Cormier and Pam Hess of the DCIIA RRC in October and November 2022 through a virtual platform. Interviewees were promised anonymity and are not identified in this report.

Industry practitioners were screened and selected using the following criteria:

- Offering financial wellness tools and services
- Active involvement with DC industry
- Significant recordkeeping line of business

Technical Note: Qualitative research is helpful in developing hypotheses surrounding a topic. However, because of the small sample size, the results described should be viewed as directional and in need of quantitative confirmation. This report is preparatory for a more in-depth study.

DETAILED FINDINGS

Data Control / Ownership

There was beginning discussion around what data is in question. Given data is sourced from many places, including payroll, investments/funds, the plan, the employer—it gets complex quickly. There is also possible data being created from the recordkeeper, independent of the plan. Further, there could be retail relationships already in existence with plan participants.

> *"Ownership is bifurcated. There is data that is ultimately sourced from a variety of sources. This is not clear-cut."*

Further, complexities exist around terminated employees. When they change their address, that is through the recordkeeper. Versus active employees, which would be done through the employer. There were many of these types of examples explored. Given this nuance,

> *"It could be that some is plan data, and some is not plan data, and they get mixed up. Where do you draw the line*?"

All recordkeepers acknowledged that the individual ultimately owns their data. The nuance between the employer and the plan sponsor/plan was clear, and all recordkeepers believe it is the employer who ultimately controls ("owns") the data—they do not believe it is a plan asset. It was noted that their contract is with the employer, on behalf of the plan, thus the data control resides there. This is in direct conflict with most employer's perspectives, and recordkeepers are clear on the implications of the differences.

> *"Most plan sponsors don't understand the intent of owning the data, but instead are using ownership to be synonymous with responsibility for."*

As this was discussed further, many recordkeepers thought if this were a plan obligation, as far as the fiduciary role is implemented, it needs to be in the best interest of the plan. And in a hierarchy, the plan comes before the individual participant.

All interviewees indicated the recordkeeper's role is to comply with directions from the plan sponsor/employer. Their job, as a recordkeeper, is to be a custodian of the assets; respond as directed and safeguard the data. The use of data is contractual, and they fulfill those obligations.

> *"We use their data in the way that they instruct us to, per their contract."*

However, it was also notable that there is broad agreement that this lack of "ownership" or custodial relationship does not reduce the legal liabilities on the recordkeeper. Recordkeepers continue to struggle with price pressure and increasing legal exposure. In lawsuits, often the recordkeeper is sought to make participants whole.

Practices and Procedures

Internal protocols were discussed, including sharing information intra-organizationally. This is being much more scrutinized, and most recordkeepers acknowledge more stringent guidelines for sharing data internally. Most indicate the need for a clear purpose and rationale, and several indicate most requests are denied internally. More internal boundaries are being put in place.

> *"Before sharing any data, there is an understanding of the critical business need and reason for the access."*

This increased scrutiny is due to litigation and recent California regulations. This has impacted their internal and external sharing of data. Sharing aggregated or non-PII data is viewed as reasonable if there is a clear benefit to the organization. There is an understanding that there is risk, so there is substantial caution to only take that risk if the value is aligned. Many also indicated that sharing de-identified information is not like "flipping a switch" this is a much more nuanced conversation. It is an operational burden, and from a risk perspective, is it de-identified enough?

> *"This is an operational burden, and we need to pull in legal, data privacy and compliance. Is there enough juice for the squeeze? What do we get out of it? We want to mitigate risk."*

Many recordkeepers discussed the data lifecycle and data tagging. Data tagging is emerging and necessary, assisting them with CPRA (California Privacy Rights Act). This is challenging but allows data to be tracked across multiple databases.

Financial Wellness Programs

> *"Financial wellness, or a holistic view of assets, is necessary so participants can make better decisions."*

Financial wellness programs continue to be prioritized across recordkeepers, with most creating strategic partnership for emerging solutions, like Emergency Savings. These add-on programs are viewed, similar to employer perspectives, as a relationship with the participant and the vendor. One recordkeeper indicated that this begins a new "chain of custody" for data.

> *"With financial wellness tools participants have to opt in, so they would have a separate relationship with the third party. Participant is still the owner, but it is more of a break in the employer/employee relationship."*

Advisor and recordkeeper relationships remain complex. Advisor requests for data at the participant or plan level continue to be debated. There are multiple challenges here, both an operational cost and a competitive cost. Many recordkeepers are competitors for advisory services. Recordkeepers indicate they will share data/send information at the behest of the employer only. However, even if the plan approves, there are also processes in place to understand the implementation cost and risk. There is a substantial amount of work involved, and it also exposes them to possible liability. The lack of standardization, and demands from many in the industry, alongside declining margins, make this a challenging conversation.

Risk and Regulatory Guidance

All recordkeepers are keenly aware of risks and liability, as recordkeepers continue to be named and exposed to lawsuits. Further, CPRA is top of mind, as this has created demands and complexity within data privacy.

> *"The state rules are like an octopus we have to maintain, with variances of rules and many tentacles."*

Many have a desire for regulatory guidance, since to date, there is no clarity. However, some worry guidance could be a "recipe for disaster." Some indicated guidance would help, if it were in the form of more use case scenarios. More specifics on what needs to be shared, and what doesn't to provide some granularity.

All indicate a standardization of data requests in the industry would be helpful. If standardization could include formats, layouts, and data elements, would make things easier across things operationally and legally. Further, many indicate the mechanism to share information is needed. Several discussed opportunities through API that would make things more secure and manageable. Standardization would also need to provide for collection, storing, sharing and disposing of data elements.

An infrastructure or data sharing consortium was also discussed, where a platform was built for connectivity and data sharing/housing. Many acknowledge the difficulties of that sort of undertaking. Getting past the minutia, all agreed it could ultimately benefit the entire industry. Most believe the barrier isn't technical. But will be privacy, legal, business challenges, and it would take time.

> *"It would take time. Healthcare didn't get where it is today in one year. It took years to get there…."*

ADVISORS/INDUSTRY PROVIDERS

Within the advisor community, individual interviews were conducted with one- to two advisors per organization across four firms. A more senior, DC-focused resource was leveraged for this process. Additionally, two additional industry interviews were held with others in the field.

In these interviews, advisors reflected on their experiences with financial wellness services, their relationship with the employer and employee, needs for participant data, permissions, challenges, and their relationships with data sharing from recordkeepers.

METHODOLOGY

The DCIIA RRC conducted six interviews across six firms. The 45-minute interviews were conducted by Warren Cormier and Pam Hess of the DCIIA RRC in October and November 2022 through a virtual platform. Interviewees were promised anonymity and are not identified in this report.

Industry practitioners were screened and selected using the following criteria:

- Organizations offering financial wellness tools and services
- Active involvement with DC plan participants
- Diversity across gender, age, and geographic locations

Technical Note: Qualitative research is helpful in developing hypotheses surrounding a topic. However, because of the small sample size, the results described should be viewed as directional and in need of quantitative confirmation. This report is preparatory for a more in-depth study.

DETAILED FINDINGS

Data Control / Ownership

Data requirements vary by advisory organization. Some rely on aggregated plan information, or less data-heavy specifics. Two of the firms fell into this category, while four indicated their desire for specifics to assist the employee with a holistic picture of their finances. Those that rely on the data believe they are constrained, and it is ultimately at the cost of participants.

> *"We don't have connections and cannot systematically get data. It is hurting participants."*

In terms of ownership or control, there are variances. Some believe it is the recordkeeper and employer, others thought it was the employer. Most advisors do not distinguish between the plan and the employer.

Advisors broadly feel limited, and recordkeeper relationships vary. There is a level of competition and increased workload for recordkeepers. Advisors acknowledge that recordkeeper margins have been squeezed, and as one advisor indicated— "how do we make one plus one equal more than two?"

For most advisors that require detailed information, it needs to be PII. This helps to improve outcomes for the end user.

For data outside the plan, that is a separate point. Most employees are willing to share information to make their experience helpful. However, it needs to be easy for them.

It is notable, all indicated that supporting individuals with decumulation, personalization is increasingly critical. Thus, data becomes even more important.

Practices and Procedures

The topic of financial wellness, most note, is complex and also not universally defined. This lack of definition creates confusion and inefficiencies.

Ideally advisors would love to have the employee be able to opt in to send information, through an intermediary.

When a relationship ends with an advisor, there are different factors that come into play on data retention, depending on the advisor, state of residence, and/or the product solution. The advisor has to retain the data for seven years, then they need to delete it. But specific products can be different.

Some financial advisors, in response to plan sponsor concerns, have begun to leverage API technology and new platforms to increase employer trust and long-term utilization.

Similar to plan sponsor feedback, advisors indicated that if recordkeepers or solutions are migrated, data can be permanently lost in the process. This speaks to the desire for standardization and connectivity in the next section.

Risk and Regulatory Guidance

With a relationship based on the individual and the size of the underlying organization, most see the risk profile of the advisor as different than that of the recordkeeper. Meaning that the recordkeeper carries a relatively risk.

All advisors agree that standardization is needed as a first step. Further, a third party, consistent and common platform would be a dramatic support. Today requests are quite varied for advisors and recordkeepers, this would help all parts of the ecosystem. A pipeline to connect data and organizations would allow for things to be (eventually) more seamless, cost effective and ultimately benefit the participant.

If a data consortium concept is executed, ideally advisors would appreciate the ability for the individual to say “yes” send this to my advisor. An opt-in, albeit seamless and simple.

ABOUT THE DCIIA RRC

DCIIA’s Retirement Research Center conducts rigorous, industry-informed research that is grounded in a practical approach focused on actionable insights. We adhere to a disciplined research methodology, governance and validation process. Our goal is to serve the industry as a reliable, unbiased, and authoritative research resource supporting improved retirement security–be it through plan design, institutional practices, investment solutions, or behavioral interventions.

To learn more, visit: **www.dciia.org/RRC**

ABOUT DCIIA

The Defined Contribution Institutional Investment Association (DCIIA) is a nonprofit association dedicated to enhancing the retirement security of America’s workers. To do this, DCIIA fosters a dialogue among the leaders of the defined contribution community who are passionate about improving defined contribution outcomes. DCIIA’s diverse group of members include investment managers, consultants and advisors, law firms, recordkeepers, insurance companies, plan sponsors and other thought leaders who are collectively committed to the best interests of plan participants. For more information, visit: **www.dciia.org**.

ABOUT SPARK

The SPARK Institute is a member-driven, non-profit organization and leading voice in Washington for the retirement plan industry. Our members include recordkeepers, mutual fund companies, brokerage firms, insurance companies, banks, consultants, trade clearing firms and investment managers. For more information, visit: **www.sparkinstitute.org.**

RRC RETIREMENT RESEARCH CENTER
A DCIIA ORGANIZATION