Chartered
Insurance
Institute

Standards. Professionalism. Trust.

Data Sharing

Unlocking outcomes: data sharing across the distribution chain

Roundtable Summary Report

cii.co.uk

Table of contents

Background

The CII is taking the lead in exploring how our sector can improve customer outcomes. This latest report follows the publication of findings from three previous roundtable discussions:

- *White Paper: Consumer Duty Board reporting*, 25 September 2024
- *The Road to Consumer Trust: Professional Standards in the Consumer Duty era*, 30 September 2024
- *Managing Vulnerability in Insurance*, 14 March 2025

We have previously identified that data sharing is insufficient both within firms and across the distribution chain which can contribute to poor customer outcomes. This issue was also highlighted by the Financial Conduct Authority (FCA)'s review of the first Consumer Duty Board Reports in December 2024, which found that many firms lacked evidence of effective data sharing with third parties. As a result, the FCA emphasised the need for firms to adopt a more comprehensive, joined-up approach to information flows throughout the product lifecycle.

Our own panellists have told us that many firms are currently experiencing challenges in sharing data or are unclear about what they should be sharing or how to monitor customer outcomes.

This roundtable was convened to address the FCA's call, with two main objectives:

- Identify the incentives and disincentives that influence the willingness and ability of firms to share information, especially where commercial sensitivities are involved.
- Identify practical steps that firms can take to overcome technical barriers for data sharing, including through the development of data sharing protocols, and assistance with governance and compliance with GDPR.

The roundtable took place on 28 May 2025.

Roundtable participants

- **Monika Banziger**, Customer Experience Specialist, Allianz UK
- **Stephanie Blenko**, Head of Policy, Association of Financial Mutuals
- **Ian Callaghan**, Director, Kingfisher Insurance. Non-Executive Director, CII Group
- **Neville Davies**, Owner, Hall Davies
- **Rachael Gagan**, Vulnerable Strategy Manager, AXA UK
- **Andrew Gething**, Managing Director, MorganAsh
- **Edward Grant**, PFS Board. CII Professional Standards Committee. Chair, Finance in Society Research Institute, University of Gloucestershire
- **Martin Grimwood**, Director, FWD Research
- **Jon Hills**, Product specialist – Conduct Risk, MS Amlin
- **Steve Kavanagh**, Director, Claim Guardians
- **Lisa Long**, Claims Conduct Consultant, RSA Group
- **Ian Munro**, Claims Governance Manager, The Acorn / Haven Insurance
- **Claire Phillips**, Chartered Financial Planner, First Wealth
- **Ian Roberts**, Contract and Controls Manager, AXA UK
- **Alan Whittle**, Director, Unburdened Solutions
- **Andrew Whyte**, CEO, Association of Financial Mutuals

- **Adam Harper**, CII, Executive Director, Strategy, Advocacy and Professional Standards
- **Vanessa Riboloni**, CII, Professional Capabilities and Insights Manager
- **Chris Shadforth**, CII, Communications Director
- **Ian Simons**, CII, Content and Capabilities Director

Framing the challenge

Insights from stakeholder engagement

Ahead of the roundtable, the CII carried out stakeholder interviews and a member survey to gather insights into some of the challenges and approaches firms are taking when sharing vulnerability data across the distribution chain. The key themes were:

- **Data capture is reactive and patchy.** Most vulnerability data are only captured at the point of claim or via direct frontline interactions, missing customers who never interact with front-line staff, whose circumstances change or who use digital-only journeys.

- **A narrow understanding of vulnerability persists.** Some practitioners still equate vulnerability with wealth or health alone, overlooking drivers such as capability, resilience and negative life events (including the distress caused by events leading to the need to make an insurance claim, which is sometimes excluded as a vulnerability flag, despite it being itself a vulnerability trigger).

- **Unclear responsibility in intermediated businesses.** There are varying views on whether and how data should pass between any and all firms in relation to a particular customer.

- **Disclosure is burdensome for customers.** Explaining vulnerable circumstances to multiple entities (or to the same firm at different touchpoints) deters disclosure by customers. Streamlining disclosures should be a design goal.

- **GDPR is a perceived to be a blocker.** Some firms are overly cautious. Explicit consent to share data is not always needed; ‘legitimate’ or ‘substantial public interest’ tests can and should apply.

- **Technical fragmentation.** Multiple CRMs and proprietary formats prevent a single view of the customer, and no sector-wide protocol exists for efficient sharing of data on vulnerability.

- **Commercial dynamics inhibit transparency.** Preserving strategic relationships across the distribution chain can inhibit whistleblowing and escalation of poor practice.

- **Incentives are defensive.** Data sharing is often framed as audit-trail protection, rather than as a vehicle for multiple firms to create customer value.

- **Trust is the keystone.** Customers will not share data unless its use and protection are clear. Likewise, firms need mutual trust and a common purpose before they will share data consistently across the chain.

During our discussion, participants added that fear is a significant and multi-layered obstacle to effective data sharing around customer vulnerability. This fear can lead to inaction or overly cautious behaviour and manifests in several ways:

- **Fear of non-compliance** with GPDR.

- **Fear of reputational damage** if data is mishandled or misinterpreted.

- **Fear among staff** about asking sensitive questions around vulnerabilities.

Scene-setting: from “problem” to “solution”

Andrew Gething, MD, MorganAsh

Andrew Gething set out a vision for a future in which vulnerability data flows “in near real-time”, saying that “if Amazon did vulnerability, they’d call it personalisation”.

People already share personal data with tech or utility companies, suggesting the public may be more willing to share than assumed. Many individuals displaying characteristics of vulnerability, especially those with disabilities, are frustrated by having to repeat their information. This is how it could work in practice:

- The first contact asks the customer’s permission to share existing vulnerability information; subsequent participants receive only what they need to fulfil the service in a tailored way, for example, share the adjustment needed, not the characteristic of vulnerability.
- Data is continuously refreshed from third-party feeds (such as death registers, open-banking).

Such sharing is in progress in utilities companies (water, gas and electricity); customers *want* this to happen as it saves them repeating trauma. Andrew stressed that 99% of the GDPR framework already permits this; what is missing are common standards and an ecosystem that promotes sharing data to create customer value, rather than meet compliance needs.

Andrew sketched four possible routes:

1. Government-mandated solution (unlikely/slow).
2. Single dominant firm’s proprietary standard.
3. Commercial providers collaborating on de-facto industry standards.
4. A CII-brokered, profession-wide standard that others can build systems around.

There are two key enablers needed to achieve this vision:

1. **Value exchange:** Customers are willing to allow their data to be shared if they believe and experience value in doing so. If firms are better able to understand personal circumstances, they can better support customers, which in turn builds trust.
2. **Data structure:** Vulnerability data needs to be structured in a way that distinguishes between the characteristic (such as, ADHD) and the required support (for example, speak to their partner), allowing the right data to be shared with the right parties.

Discussion: exploring solutions

Our roundtable discussion focused on identifying practical solutions to the challenges identified. These fell into eight themes:

1. Cultural shift: from compliance to outcomes

There is a need to reframe data sharing as a commercial opportunity rather than a compliance burden. This involves moving beyond the “regulatory stick” to the “loyalty carrot” that results from providing a more personalised, effective service, which can only be achieved through efficient and secure data management within and between firms.

2. Standardisation is essential for interoperability

It is necessary to create a standardised taxonomy for vulnerability and agree sharing protocols. Without common definitions and data structures, firms interpret and handle vulnerability data inconsistently. Participants called for a shared language and framework that all parties across the distribution chain can use.

3. Empowering intermediaries

Brokers and advisors are crucial in identifying and managing vulnerability due to their close relationships with clients. They often act as informal “data custodians”, helping to pass on relevant information to manufacturers and other parties. However, they need the right systems, standards, guidance, and support to improve data flows across the value chain.

4. Giving customers control over their data

Customers must be able to access, update, and control their data easily to feel safe and empowered. One solution might be a single consumer-controlled “data passporting” repository, where individuals share their vulnerability information and firms access what they need. This was likened to the “Tell Us Once” bereavement service. Such a system might face challenges around cyber-security, while there is currently a lack of a central authority to manage such a system.

5. The potential of AI

AI was proposed as a technology that could be used to help infer vulnerability from behaviour and communications, and to monitor compliance. Concerns about potential algorithmic bias, potential erosion of trust if perceived as “spying”, and the need for human oversight over AI outputs were noted. An effective approach to identifying vulnerability would combine inferred data with voluntary disclosures from customers to build a fuller, more accurate picture. This dual approach respects customer agency while enhancing support capabilities.

6. Education and guidance

There was strong consensus that the CII has a leading role to play in driving professional awareness about the need for wider understanding about the benefits of collecting and sharing vulnerability data. A key element in this could be embedding vulnerability into its qualifications and CPD resources.

There was also a strong call for consistent guidance on interpreting GPDR in the context of vulnerability data management. The CII is already developing guidance in this area.

Discussion: exploring solutions

7. The “value exchange” must be made clear

Customers need to see tangible benefits from sharing their data (for example, better service or tailored support) and firms must demonstrate that data is used ethically and effectively, not just collected for compliance. Firms need to promote the ways they can support customers, as customers may not know what help is available or that they are vulnerable. There was a suggestion to explore “customer marks” or other forms of recognitions for firms demonstrating good practice in supporting vulnerable customers.

8. Inclusive design

It is essential to involve consumers in shaping next steps and developing standards, especially those with lived experience of vulnerability. This would ensure that solutions are grounded in real needs rather than assumptions. A key outcome must be solutions that tackle digital exclusion and are universally accessible.

Conclusion and next steps

The roundtable concluded that progress in data-sharing across the distribution chain requires both technical solutions and a significant shift in cultural mindset on the part of many firms who should focus more on the benefits to customers and the wider system from greater data sharing.

It is apparent that no single organisation can solve these challenges alone. There was a loud call for collaboration between regulators, professional bodies, trade associations, consumer groups, and platform providers. Attendees suggested that these organisations should work together to develop shared standards, guidance, and incentives for data sharing. The CII intends to drive collaboration by creating focused working groups to develop targeted guidance and solutions for specific value chain areas (like intermediated versus direct models).

Next steps

The CII has a key role in normalising behaviours and promoting best practices across the sector. We intend to:

- **Lead stakeholder collaboration:** Convene a cross-sector working group (including consumers) to co-develop solutions for some of the challenges identified. A key focus will be on the creation of a common vulnerability taxonomy. This group may also form tailored subgroups to address the distinct needs of different sectors, such as insurance and financial planning.

- **Enhance Professional Standards:** Integrate vulnerability content within CII qualifications and Continuing Professional Development (CPD).

- **Publish vulnerability management and GDPR guidance:** Soon to launch, the CII is developing good practice guidance on how to manage vulnerability and measure outcomes to meet regulatory requirements, as well as guidance on managing vulnerability data while remaining GDPR compliant.

- **Conduct lived experience research:** Gather insights from individuals who have lived experience of vulnerability, to inform the development of our guidance, shape case studies, and help craft compelling narratives that clearly illustrate the benefits derived from better managing vulnerability.

Chartered
Insurance
Institute

Standards. Professionalism. Trust.

Unlocking outcomes: data sharing across the distribution chain

Roundtable Summary Report