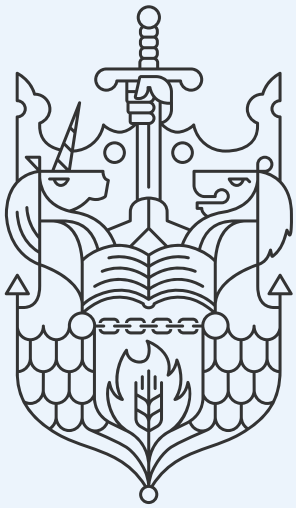

Chartered
Insurance
Institute

Standards. Professionalism. Trust.

Vulnerability data sharing

Roundtable summary report

Vulnerability Data Sharing Taskforce - Session 1
3 March 2026

Contents

As a chartered body with a public interest mandate, the Chartered Insurance Institute provides a forum where stakeholders can collaborate on shared challenges. Our independence enables honest dialogue, facilitating the development of sector-wide guidance and recommendations that strengthen professional standards and deliver better customer outcomes.

Executive summary

The CII convened regulatory, sector, technology, academic and lived experience experts to examine how vulnerability data is shared across the insurance and personal finance distribution chain, exploring the opportunities, barriers and design choices that emerge when firms try to share information responsibly.

The Financial Conduct Authority (FCA) Consumer Duty (FG22/5) and guidance on treatment of customers in vulnerable circumstances (FG21/1) set a clear expectation that firms evidence good outcomes for customers in vulnerable circumstances across the entire distribution chain. Yet current data sharing remains fragmented, reactive and inconsistent. Customers are routinely asked to repeat sensitive disclosures, and information that already exists within the market often fails to follow them across the value chain.

Participants agreed that UK GDPR is not, in itself, the barrier many firms perceive it to be. The legal framework permits responsible data sharing where there is a lawful basis, transparency, purpose limitation, data minimisation and proper accountability. The *Joint FCA and Information Commissioner's Office (ICO) statement on regulatory expectations regarding firms' approaches to vulnerability related data* [Link] corroborates this position.

Progress has instead been held back by the absence of common language and standards, by uncertainty and risk aversion, and by fragmentation across distribution chains, manufacturers and intermediaries.

Three speakers presented current models in practice: the Experian Support Hub, which standardises support needs across organisations under consumer control; FWD's research with commercial lines insurers and brokers, demonstrating that collaboration across the distribution chain is achievable when capability, opportunity and motivation are addressed together; and Morgan Ash's analysis of the wider landscape, drawing on the Priority Services Register precedent in utilities.

The discussion surfaced design tensions around how a common taxonomy should be structured, whether support needs or underlying circumstances should be primary, how customer consent and control should operate in practice, and where responsibility for initiating data sharing sits within the value chain.

Participants agreed that the taskforce should focus on practical progress rather than theoretical debate, anchored in clear customer journeys where data sharing can demonstrably improve outcomes. Three working groups were established to take forward taxonomy and definitions, market adoption, and data standards and governance.

The CII is committed to facilitating the co-creation of practical, sector-wide resources and to convening the cross-sector dialogue needed to make vulnerability data sharing a reality.

Introduction

The FCA's Consumer Duty (FG22/5) and guidance on treatment of customers in vulnerable circumstances (FG21/1) require firms to evidence consistent delivery of good outcomes for all customers. The regulator's December 2024 review of Consumer Duty Board reports [Link] found insufficient evidence of firms sharing appropriate information across the distribution chain, a finding that makes the case for collective action.

In May 2025, the CII convened a roundtable focusing on data sharing across the distribution chain [Link], as part of its Road to Consumer Trust campaign. Participants called for the CII to convene a cross-sector working group to develop a common vulnerability taxonomy and supporting standards.

This paper summarises the discussion from the first session of the resulting Vulnerability Data Sharing Taskforce, held on 3 March 2026.

Framing the challenge: from compliance to outcomes

The roundtable opened by inviting participants to consider what the sector should share in order to improve outcomes for vulnerable customers. The shift from a compliance lens to an outcomes lens was a recurring theme throughout the session.

The discussion raised the following observations:

- **Vulnerability information is rarely held in any single place.** A customer's life and financial footprint typically span multiple organisations, and the distribution chain itself splits relationship, product and service responsibilities across manufacturers, intermediaries and service providers.
- **"Data sharing" means different things to different organisations.** For some it implies the structured transfer of records between firms; for others it describes signals, indicators or customer-authorised access across systems. An early action for the taskforce will be to agree a clear working definition.
- **Customers are often frustrated by being asked to repeat disclosures.** Participants challenged the assumption that customers do not expect data to be shared between firms acting on their behalf.
- **Regulatory and market developments favour data sharing.** Consumer Duty, the evolution of Priority Services Register ecosystems and the Data (Use and Access) Act 2025 point towards a sector that takes vulnerability and customer-controlled data more seriously.

Participants agreed that the taskforce should focus on practical progress rather than theoretical debate, anchored in use cases that demonstrably improve outcomes.

GDPR and data sharing fundamentals

One attendee invited participants to think about UK GDPR not as a compliance hurdle but as a reflection of how customers reasonably expect to be treated. The principle is intuitive: a customer who shares sensitive information with one organisation expects that information to be handled with care and not passed on without their knowledge.

Sharing data is itself a form of processing, so any data sharing must satisfy the same principles that apply to data collection. The key principles relevant to vulnerability data sharing include:

- A lawful basis for processing under Article 6 remains required, such as contractual necessity, legal obligation, vital interests or legitimate interests.
    - In addition, the CII recommends applying an Article 9 condition as a default position, treating all vulnerability-related data as Special Category Data to ensure a consistently high standard of protection, governance and accountability.
- **Transparency** with customers, supported by clear privacy notices and direct communication, so that customers understand their data may be shared and with whom.
- **Purpose limitation**, ensuring data is shared only for the purpose for which it was originally collected.
- **Data minimisation**, sharing only what is necessary for the intended purpose.
- **Accountability**, supported by data protection impact assessments, governance processes and appropriate documentation.

The joint FCA and ICO statement reinforces that data protection law should be seen as an enabler, not a barrier, to supporting customers in vulnerable circumstances. It makes clear that firms can share personal and even special category data where necessary to deliver good outcomes, provided they do so lawfully, fairly and transparently in line with UK GDPR principles.

Crucially, the statement highlights that failing to share relevant information can itself lead to poor outcomes, encouraging firms to take a more confident, outcomes-focused approach to vulnerability data sharing across the distribution chain.

When this approach may not be optimal

Special Category Data must be managed under Article 9 of UK GDPR, which imposes stricter requirements than Article 6 (which governs 'ordinary' personal data). In some circumstances, applying Special Category Data standards may be more onerous than necessary.

Bereavement, which is not considered Special Category Data, provides a clear example. The immediate priority in this scenario is providing sensitive, timely support rather than obtaining explicit consent, which in these circumstances would create unnecessary delays and add distress.

Firms with established bereavement support processes designed around Article 6 requirements (such as legitimate interests) may reasonably continue using those processes without requiring explicit consent.

UK GDPR does not block responsible vulnerability data sharing.

The data and how it is managed must be architected in a way that is compliant with GDPR principles. Where firms have built systems and processes around lawful basis, transparency and minimisation, they have been able to share. What is missing is a common standard with respect to sharing.

Vulnerability data sharing in practice: Three perspectives

Three speakers shared current models and research, illustrating the spectrum of approaches now active in the market.

Experian Support Hub - Dr Chris Fitch

Dr Chris Fitch from the Money Advice Trust and the University of Bristol described the Support Hub initiative, which standardises support needs across multiple organisations under explicit consumer consent and control.

Three observations stood out:

1. There is no single way to share vulnerability data: pooled databases, temporary access models and firm-to-firm exchanges all play different roles, and a workable sector approach will likely combine more than one.

2. What consumers consistently ask for is transparency about how their data is used, control over who it is shared with, and confidence in the security protections around it.

3. Models often described as "single registers", such as the Priority Services Register in utilities, are in practice many separate implementations; uniformity at the surface can mask fragmentation underneath. This was highlighted in Chris' recent publication, 'Tell us ~~Once~~: Twenty' report [Link].

The Data (Use and Access) Act 2025 was flagged as a development that strengthens consumer data portability rights and may, over time, allow individuals to set up their own data-sharing networks across firms.

This applies to both personal and special category data, although the latter is subject to a higher bar, requiring additional safeguards, lawful conditions and more rigorous governance to ensure it is handled appropriately.

Insurer-broker collaboration - Martin Grimwood

Martin Grimwood of FWD Research provided details of a two-year research project with commercial lines insurers and brokers. Given a long-standing reluctance of brokers to allow insurers to access their customers for market research purposes FWD piloted a new approach that encouraged brokers and manufacturers to collaborate on vulnerability data sharing.

FWD's research used a behavioural change framework looking at three drivers:

1. **Capability,** whether firms have the knowledge and skills to act;

2. **Opportunity,** whether legal, regulatory or competitive concerns create barriers; and

3. **Motivation,** whether firms see commercial as well as regulatory benefits in addressing vulnerability.

The conclusion was that collaboration is achievable where the right safeguards are in place, and that attitudes are shifting as firms increasingly recognise that addressing vulnerability has commercial as well as regulatory benefits.

The wider landscape - Andrew Gething, MorganAsh

Andrew Gething of MorganAsh focused on practical considerations across the value chain. Customers interact with multiple organisations across financial services and utilities, yet vulnerability data is rarely shared between them. The Priority Services Register in energy demonstrates that individual-level vulnerability data can be shared at scale.

Customers can find themselves frustrated when they have to repeat the same information to firms working on their behalf. The argument for an incremental route, such as building interoperability between existing players rather than waiting for a single centralised database, was suggested the most likely path to deliver progress.

Several areas were flagged as critical for the taskforce to address taxonomy structure, severity indicators, support needs classification, governance frameworks, and technical standards for data exchange. The point was made that technology is not the primary barrier; organisational priorities and a lack of cross-firm coordination are.

The core debate: structural and design tensions

The discussion surfaced three areas of tension.

Taxonomy design: support needs versus circumstances

A central design choice is how a common taxonomy should be structured. Three approaches were considered:

- **Support needs as the primary structure**, with circumstances secondary. Information is captured in terms of what the customer needs (for example, communication adjustments, additional time, written follow-up) rather than why. This is the model the Support Hub uses.
- **Circumstances as the primary structure**, with support needs secondary. Information follows the underlying driver of vulnerability (for example, life events, financial disruption, health) and support needs are derived from the circumstance.
- **Parallel structures where both are treated equally.** Circumstances and support needs are recorded alongside one another, allowing different organisations to use whichever is most relevant to their service.

The taskforce agreed that starting with practical use cases, such as new business or claims journeys, would help guide the choice.

Customer disclosure, consent and control

The discussion surfaced a recurring tension between consumer control of data and the operational complexity of obtaining meaningful consent. Customers want transparency, control, and security, but consent fatigue is real and requiring detailed disclosure risks making the customer experience worse.

Two design ideas were discussed in this context.

1. The idea of a “support menu” that organisations can offer to customers without requiring disclosure of specific vulnerability characteristics. The customer selects the adjustments they want, and the firm acts on these preferences.

2. The second is the principle that customers should remain in control of who their data is shared with, how long it is held, what level of detail is shared, and how often it is reviewed.

Participants noted that framing matters. If data sharing is positioned as something done to the customer for the firm's benefit, trust disappears. If it is positioned as something done with the customer to spare them repeated disclosures and to deliver more consistent support, the conversation changes.

Where responsibility sits across the distribution chain

Manufacturers, intermediaries, and service providers each hold a partial view, and it is often unclear where responsibility for initiating data sharing should sit. Brokers have historically held the customer relationship and have been reluctant to share insight with manufacturers; manufacturers in turn have limited visibility of customer circumstances at the point of sale.

Participants noted that any successful approach will need to work across organisations of varied sizes and operating models. A standard that is workable for a large insurer but unworkable for a small broker (or vice versa) will not achieve sector adoption.

From theory to practice: governance, adoption and implementation

The discussion turned to how the taskforce can move from principles to practical adoption across the sector. The following guiding principles emerged:

1. **Start with use cases.** Concrete customer journeys (for example, new business, claims, complaints, lapsing customers) give the taskforce a way to test whether any proposed approach improves outcomes.

2. **Prioritise outcomes over efficiency gains.** The primary measure of success must be improved outcomes for vulnerable customers, not the operational savings firms might achieve along the way.

3. **Leverage existing standards and initiatives.** Frameworks already exist in adjacent sectors. The taskforce should build on these rather than starting from scratch.

4. **Design for proportionality.** Any standard must be implementable by organisations of different sizes and operating models if it is to achieve sector-wide adoption.

Participants surfaced the following considerations across three phases of work:

Phase	Considerations
Taxonomy and definitions	*What should a common taxonomy capture?* The taskforce will need to decide whether support needs or circumstances are the primary structuring logic, what level of detail is appropriate for a Draft 1.0, how the taxonomy can handle change over time, and how language and definitions are chosen to support consistency without losing nuance. Practical use cases should anchor these choices, and the taxonomy should be oriented towards informing decisions and outcomes rather than producing labels.
Market adoption and engagement	*What gives firms the confidence to adopt?* Different audiences respond to different drivers, so the narrative will need to combine consumer outcomes, commercial benefits, and professional leadership. Participants suggested identifying a small number of pioneer organisations willing to test the framework in practice.
Data standards and governance	*What technical and governance scaffolding is needed?* Common technical standards (such as data structure, transfer protocols, severity indicators, and support needs classifications) are a prerequisite for interoperability between existing systems. Governance arrangements need to address approval standards for firms accessing shared data, security expectations, and how the standard is maintained and evolved over time. The principle of customer control should be designed into the technical architecture.

Measuring success: monitoring for genuinely better outcomes

Outcome monitoring is a core requirement of the Consumer Duty, and the same principle applies to any sector-wide data sharing standard. Several measurement principles were raised:

- **Customer experience indicators**, including reductions in repeated disclosures across the distribution chain and customer-reported confidence that their support needs are understood.
- **Outcome differentials** between vulnerable and non-vulnerable customers, used as a test of whether the framework is closing rather than widening gaps.
- **Adoption indicators** across firm types, ensuring the standard works for small intermediaries as well as large manufacturers.
- **Governance and accountability**, for example, clear ownership of monitoring, escalation pathways when concerning patterns appear, and the ability to conduct root cause analysis when adverse outcomes occur.

Measurement design should therefore be considered from the outset.

Conclusion and next steps

The first session of the Vulnerability Data Sharing Taskforce confirmed the appetite across the sector for a practical, outcomes-driven route to better vulnerability data sharing.

Three working groups were established at the close of the session to take this work forward:

- **Taxonomy and definitions:** developing a Draft 1.0 of a common vulnerability taxonomy, including principles, structure, and language.
- **Market adoption and engagement:** building the strategy to secure sector-wide confidence, identify pioneer firms, and create visible momentum.
- **Data standards and governance:** beginning work on technical and governance standards for data structure, transfer, and controls.

Our independence as a Chartered body enables us to convene the cross-sector dialogue needed to develop sector-wide solutions that strengthen professional standards and deliver better outcomes for customers in vulnerable circumstances.

Appendix: resources

Regulations

- 'Data (Use and Access) Act 2025 (c. 18)', *Legislation.gov.uk* (Crown Services, London 2025 [Link]
- 'Data Protection Act 2018 (c. 12)', Legislation.gov.uk (Crown Services, London 2018 [Link]
- Financial Conduct Authority, FG21/1 *Guidance for firms on the fair treatment of vulnerable customers* (FCA, London 2021) [Link]
- Financial Conduct Authority, *FG22/5 Final non-Handbook Guidance for firms on the Consumer Duty* (FCA, London 2022) [Link]
- Financial Conduct Authority, *Joint FCA and ICO statement on regulatory expectations regarding firms' approaches to vulnerability related data* (FCA, London 2026) [Link]
- *Regulation (EU) 2016/679 of the European Parliament and of the Council*, Legislation.gov.uk (Crown Services, London 2016) [Link]

Frameworks and standards referenced

- Ten Principles for Designing Vulnerable Customer Data Sharing Approaches
- Support Needs Taxonomy and the Experian Support Hub
- Priority Services Register (utilities)

CII publications

- Chartered Insurance Institute, Managing customer vulnerability in insurance and personal finance, a practical implementation guide (CII, London 2025) [Link]
- Chartered Insurance Institute, Unlocking outcomes: data sharing across the distribution chain (CII, London 2025) [Link]
- Chartered Insurance Institute, Artificial Intelligence and vulnerable customers (CII, London 2025) [Link]

Participants

Name	Organisation
Rebecca Aston	Chartered Insurance Institute (CII)
Julie Arthy	Chartered Insurance Institute (CII)
John Bissell	Chartered Institute of Loss Adjusters (CILA)
Rob Bell	RB Compliance
Hannah Bradley	Chartered Insurance Institute (CII)
Carla Brown	Personal Finance Society (PFS)
Alan Clay	LexisNexis Risk
Hannah Coffey	St. James's Place
Eddie Grant	Chartered Insurance Institute (CII)
Richard Groom	Chartered Insurance Institute (CII)
Andrew Gething	MorganAsh
Martin Grimwood	FWD Research
Adam Harper	Chartered Insurance Institute (CII)
Toni Hatton	The Exeter
Dan Holloway	Rogue Interrobang
Emily Kenna	SenseRisk
Jan Levy	Three Hands
Hannah Murphy	Royal London
Amanda Nicoll	Advent RTA Ltd
Vanessa Riboloni	Chartered Insurance Institute (CII)
Julia Richardson	Davies Group
Kelly Spier	Just
Sophie Spencer	T L Dallas & Co Ltd
Craig Tracey	Brabazon Solutions
Ralph Tucker	Empath AI
Charlie Williams	CXCo
Christopher Finch	University of Bristol
Nick Green	Criterion
Ron Wheatcroft	Swiss Re
Niamh Collinge	AJ Bell

Chartered Insurance Institute

Vulnerability data sharing
Roundtable summary report