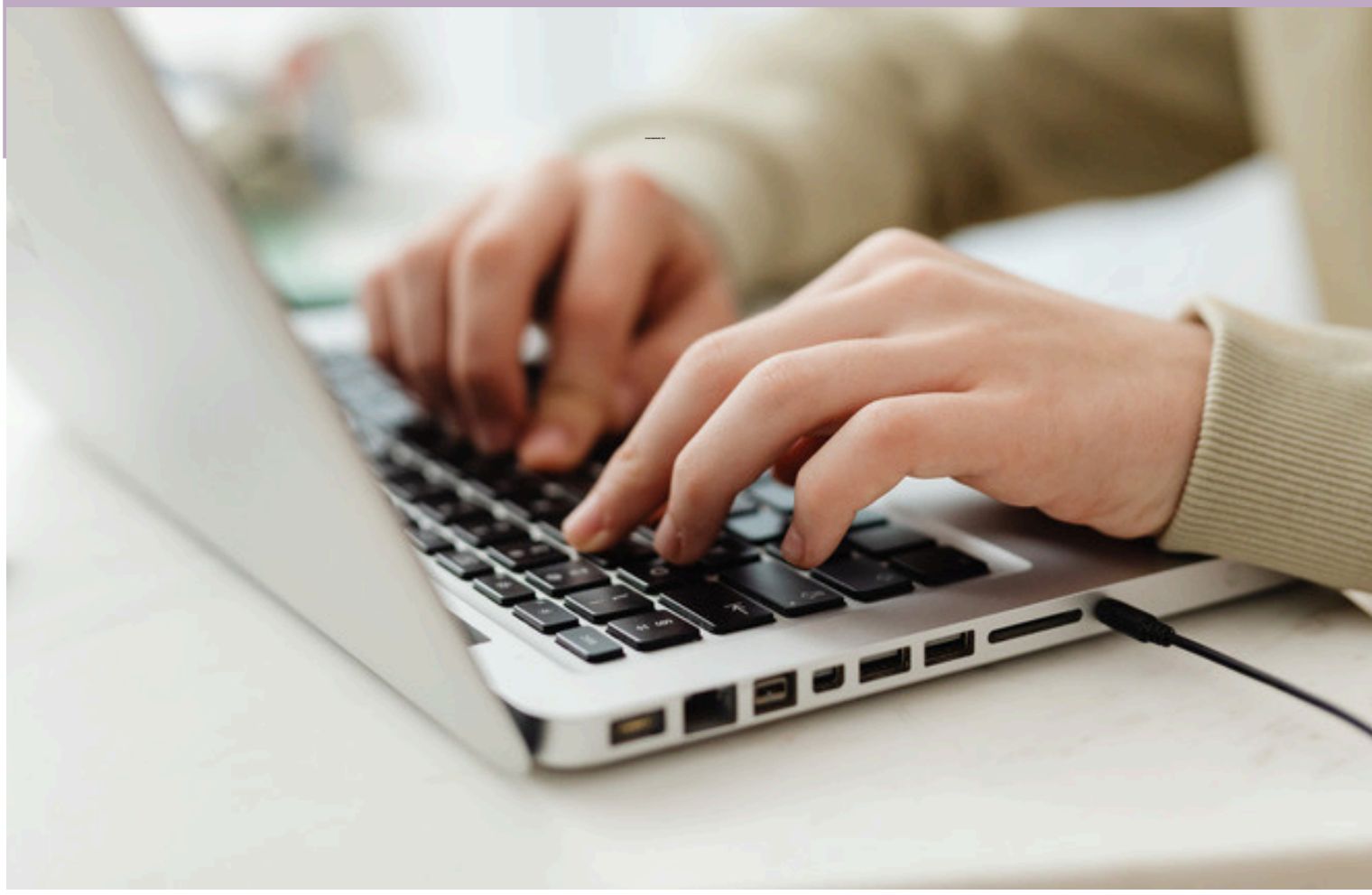
Financial Vulnerability Taskforce

CONSUMER DUTY ALLIANCE

A SAFE PAIR OF HANDS

How to record information about clients in vulnerable circumstances

A good practice guide and checklists



In partnership with Fintect

The aims of this guide

This guide explains how to record, store and use information about clients who may have a characteristic of vulnerability, in a way that is lawful, respectful and proportionate. It helps firms meet their duties under FCA Consumer Duty, UK GDPR and the Data Protection Act 2018. It does not cover how vulnerabilities are identified or assessed, which will require separate guidance, training and judgement.

The aim is to protect clients, support good outcomes and reduce risk for your firm.

If recorded properly this information can:

- Improve outcomes for clients
- Meet FCA Consumer Duty expectations
- Comply with data protection law
- Protect your firm from complaints, SARs and enforcement action.

Well-kept records are important

The FCA expects firms to identify vulnerable clients and monitor whether they are receiving appropriately differentiated and equitable client service and outcomes.

In addition, data protection law has strict rules on how this information is used.

Poorly recorded vulnerability information is a common cause of complaints, Subject Access Requests, and supervisory challenge, even where firms have acted with good intentions.

Conversely, well-kept records and carefully considered procedures can lead to:

- Better client outcomes
- Enhanced customer satisfaction and increased referrals
- Well-presented examples of working with vulnerable clients if requested by the FCA.

The FCA's view of vulnerability

The FCA says vulnerability usually falls into one of four main areas:

HEALTH

- Physical or mental health conditions
- Cognitive decline
- Neurodivergence
- Addiction
- Sensory impairment (sight, hearing, etc).

LIFE EVENTS

- Bereavement
- Job loss
- Relationship breakdown
- Retirement
- Increased caring responsibilities
- Financial abuse or coercion.

RESILIENCE

- Difficulty coping with financial or emotional shocks.

CAPABILITY

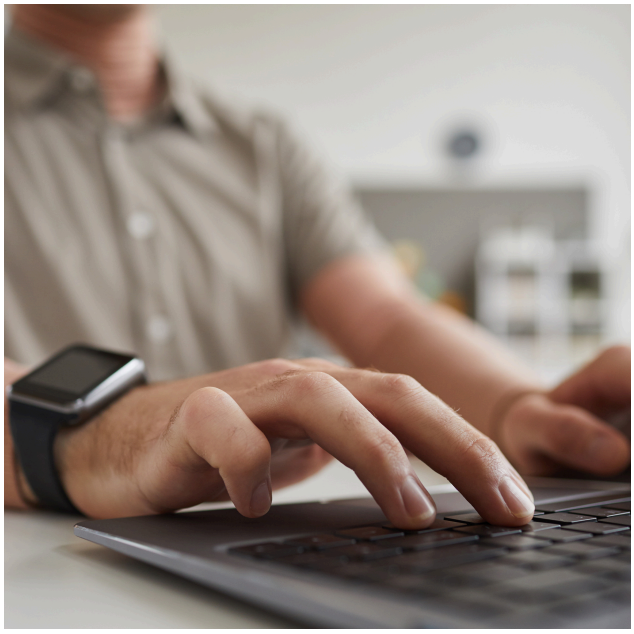
- Low financial knowledge
- Low digital skills
- Language barriers
- Lack of confidence with managing money.

Key data protection rules

When recording vulnerability information it must be:

- Collected for a clear reason
- Relevant and not excessive
- Handled and used lawfully and fairly
- Accurate and kept up to date
- Stored securely
- Kept only for as long as needed
- Easy to explain and justify, if asked.

Firms should be able to clearly explain why each category of vulnerability information is recorded, how it supports good client outcomes, and why holding that information is necessary and proportionate, rather than recording information "just in case".



Handling sensitive personal data

Some vulnerability information will be classed as Special Category Data (SCD) under UK GDPR, especially:

- Health information
- Disability information
- Mental capacity or cognitive issues.

This type of data requires:

- A clear legal basis for collecting and using it (often explicit consent)
- Extra security
- As little detail as possible.

Not all life events (e.g. bereavement or job loss) are Special Category Data, but they must still be handled carefully.

Where vulnerability information relates to health, neurodiversity or special educational needs and disabilities (SEND), records should avoid unnecessary medical detail. Instead, focus on how the client's communication, understanding and support needs are impacted.

Good practice when recording vulnerability

DO.....

- Tell clients why you are recording the information (usually via your privacy notice or client terms)
- Get explicit consent for recording Special Category Data
- Use the client's own words wherever possible or neutral/factual language
- Record only what you need
- Clearly state whether information is fact or opinion
- Record who provided the information
- Review and update records regularly - especially where circumstances are temporary, evolving or context-specific
- Use secure systems with access limited to staff who need it to fulfil their job role or because they are customer-facing
- Train staff in both vulnerability and data protection
- Write records on the assumption that the client, the FCA or the ICO may read them
- Focus on how a client's circumstances affect their understanding, decision-making or ability to engage, rather than applying labels or diagnoses
- Consider signing up to the Vulnerability Registration Service, which can identify clients who have registered a vulnerability, help you to support them as part of the partnership network, and flag clients who may benefit from being registered
- Be clear internally how recording this information supports good client outcomes and regulatory compliance.

Good practice when recording vulnerability

DON'T....

- Record unnecessary or excessive detail
- Use judgemental or emotional language – use correct medical terms if you can
- Make clinical or capacity assessments
- Write long free-text notes that could be misunderstood
- Assume clients will never see the record
- Record information that cannot be clearly justified as necessary for delivering appropriate advice or service
- Assume that a vulnerability automatically limits a client's capacity to make decisions

Use codes to reduce risk

Where possible, using codes or categories instead of detailed notes helps to reduce risk.

You can record:

- Type of vulnerability (maybe use letters)
- Severity or level (maybe use numbers that are appropriate based on medical, quantitative references)
- Source (client-provided or firm's opinion).

Consider using a customer reference number, instead of names to anonymise the data further.

All of this will:

- Reduce the amount of data held
- Lower risk from a SAR
- Improve consistency and reporting
- Reduce risk of using inappropriate language.

Coding and categorisation can be especially helpful for smaller firms that want to reduce risk without creating complex systems. They can also help firms avoid over-interpretation, particularly where circumstances are changing or where the client's situation does not require ongoing support.

Keep vulnerability information secure

You must make sure that:

- Only authorised staff can see vulnerability information
- Electronic systems are protected by passwords and/or MFA
- IT systems are kept up to date with security patches
- Paper records are locked away
- Paper and electronic records are destroyed securely when no longer needed.

What Subject Access Requests (SARs) mean for you

Clients have the right to see their personal data including:

- CRM notes
- Emails and messages
- Meeting notes, if stored electronically
- Vulnerability records

Remember:

- Always write notes as if the client will see them
- Language that is vague, emotive or interpretive is more likely to be misunderstood or challenged when disclosed
- Client-provided information must be shared
- Firm opinions may have to be disclosed unless a specific exemption applies
- Using codes and limited detail or anonymisation reduces risk
- Staff must know how to recognise and escalate SARs promptly

Training and responsibility

Firms should appoint a data protection lead (internal or external) and ensure staff are trained to:

- Identify signs of vulnerability
- Record information correctly and respectfully and explain and justify why it has been recorded if challenged.
- Know how to spot and escalate a SAR
- Not assume responsibility for data protection compliance lies with the networks or compliance providers – every firm has this legal duty

The depth and formality of training and record-keeping should be proportionate to the size, nature and complexity of the firm and its client base.

More information on SARs in relation to SMEs can be found on the ICO website.

For larger organisations, visit this page.

“Always write notes as if the client will see them”

Key takeaways

When in doubt: record less, record carefully, and be transparent.

Ask yourself “Would I be happy for the client or FCA to read this?”

Adviser prompt (use every time):

- Do we need this for advice or support?
- Have we explained why?
- Is it minimal, factual, and recorded in a way the client would be comfortable reading?

Handling Sensitive Information

A Five Step Flow

1

Explain and agree

Explain what you need, why, and how it will be used. For sensitive info, ask for explicit permission.

2

Collect only what's needed

Gather only relevant information. Avoid unnecessary detail - focus on what helps serve the client and don't keep information 'just in case'.

3

Record clearly and respectfully

Use the client's own words or neutral language. Note who provided it, the date, and whether it's fact or opinion.

4

Protect and limit access

Store in secure systems. Restrict access to trained staff. Apply extra safeguards for sensitive data.

5

Review, update and delete

Review regularly, update when circumstances change, and delete when no longer needed.

A SAFE PAIR OF HANDS

DATE: _____

NAME: _____

CHECKLIST FOR BUSINESS OWNERS	☑
Do clients understand why we record vulnerability information?	
Do we get client consent for Special Category Data?	
Are we recording only what's necessary?	
Do we handle sensitive data with extra care?	
Could we respond confidently to a SAR?	
Are staff trained and supported in how to identify vulnerability and record it?	
Is access to data properly restricted?	

This checklist should be reviewed and completed at least annually, and whenever significant changes occur within the business, including the recruitment of a large number of employees, the implementation of new IT systems, or changes to data collection, storage, or processing procedures.

Financial Vulnerability Taskforce
CONSUMER DUTY ALLIANCE

A SAFE PAIR OF HANDS

DATE: _____

NAME: _____

CHECKLIST FOR STAFF	☑
Is this information necessary?	
Is it factual and respectful?	
Have I used minimal detail?	
Could the client read this without concern?	
Is access to this record restricted?	

This checklist should be completed when creating a new client record or updating an existing client record.

Financial Vulnerability Taskforce

CONSUMER DUTY ALLIANCE

A SAFE PAIR OF HANDS

In partnership with Fintect

Data protection specialists for financial services firms