THE OFFICE OF THE
Data Protection Authority

THEMATIC REVIEW REPORT

2025-2026

SCOPE OF REVIEW:

On the processing of personal data through the 'Medicus Case Management System' by Guernsey-based GP practices

THE OFFICE OF THE Data Protection Authority

Contents

Contents 2
1. Foreword 3
2. What is a Thematic Review? 3
3. Why this review was initiated 4
4. How the review was conducted 5
Stage 1: Initial Engagement 5
Stage 2: Assessment 5
Stage 3: Feedback 6
5. General findings 6
5.1 Positive observations 6
5.2 Areas requiring improvement 6
6. Outcomes 8
7. Key takeaways 9
8. Conclusion 11

1. Foreword

Healthcare providers are a vital part of our community in the Bailiwick of Guernsey. Individuals rely on their services for necessary medical treatment, and in doing so, provide these organisations with their personal data. In carrying out their functions, they generate further information about their service users, much of which is sensitive medical information, and this is recorded and logged internally to support the delivery of care.

Under the Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law"), medical information is designated as Special Category Data, requiring the organisation (also known as the "controller" under the Law) to apply additional measures and safeguards to better protect it.

The Data Protection Authority ("the Authority") is responsible for regulating the processing of personal data by controllers, such as healthcare providers, to ensure information is being handled lawfully, transparently and fairly.

> *"Thematic reviews play a critical role in identifying risk areas before they translate into real-world harms, which is especially important in a sector such as healthcare where organisations are responsible for some of the most sensitive personal data."*
>
> Brent Homan, Commissioner for the Data Protection Authority

This thematic review focused on the use of a digital case management system ("Medicus"), shared between three local GP practices, who in turn oversee multiple surgeries. These practices are:

- IslandHealth
- Healthcare Group
- Queen's Road Medical Practice

This report details the findings of this review. In sharing these findings with the public, the Authority provides transparency about its activities to ensure compliance and, importantly, offers practical guidance that other organisations within the Bailiwick can consider when reviewing their own processes.

2. What is a Thematic Review?

The Authority has a range of tools available to raise the level of compliance within a sector. This includes formal sanctions, such as fines at one end of the spectrum, to informal resolutions at the other. One of these tools is a thematic review. The goal of a thematic review is to identify a relevant sector, group or organisation within the Bailiwick of Guernsey that processes the personal data of Bailiwick residents, whether at a high volume, of a sensitive nature or both. Focusing on a specific aspect of the processing, the Authority then assesses compliance and provides guidance and support to help those organisations improve their processes and ensure compliance with the Law.

This allows the Authority to engage with industry broadly and at the ground floor, reducing the likelihood of data protection issues arising in the future.

Thematic reviews are a non-formal enforcement tool as opposed to a formal investigation that arises from the receipt of a complaint or breach report. To that end, they rely on the good faith efforts of organisations to cooperate with the review, and given their voluntary and sector-wide nature, result in lower costs and disruption than a formal enforcement action.

As a result, organisations with a genuine commitment to compliance with the Law often choose to participate in these reviews and work collaboratively with the Authority to identify and address any gaps in their compliance framework. In doing so, they also benefit from access to the Authority's expertise and regulatory insight.

The Authority publishes the outcomes of thematic reviews to inform the public and other organisations of any relevant findings and better support the wider community in meeting their requirements under the Law.

3. Why this review was initiated

During its engagement with the GP practices listed above, the Authority became aware of a shared case management system known as Medicus, which is used by several GP surgeries to manage patient records.

Within Medicus, access to patient records is carefully controlled. When a patient registers with a GP practice, only that organisation and the out-of-hours service can access their records on the system.

Access is ringfenced. Other GP practices can only access those records if the patient registers with, or transfers to that organisation. Following a transfer from a practice using Medicus the previous records are made inactive, limiting the former practice’s access to specific and extenuating circumstances.

The Authority was cognisant of the features of such a shared system and the importance of implementing appropriate technical and organisational measures to facilitate lawful access and sharing of patient data. This can impact processes outside of routine business activities, such as the receipt of Data Subject Access Requests (DSARs), therefore, it is important any organisation using such a system has clear guidelines on how to handle requests.

Taking into consideration the special category medical data processed by GP practices, the Authority determined a thematic review would be a beneficial exercise and reached out to the three practices. All three engaged positively with the review and welcomed the opportunity to receive additional guidance and support.

The scope of the review focused on the governance surrounding Medicus, including but not limited to:

- The retention period(s) of personal data processed through Medicus
- Appropriate use of Medicus by the GP practice and its staff
- Access privileges and corresponding roles/responsibilities within the organisation
- Facilitation of data subject rights, such as Data Subject Access Requests

- Informing customers of the processing (including sharing) of their personal data through Medicus

4. How the review was conducted

The thematic review was broken up into three distinct stages, designed to simplify the process:

1. **Engagement phase**
2. **Assessment phase**
3. **Feedback phase**

Following the review, the GP practices actioned the recommendations generated during the feedback phase, within an agreed timeframe.

Stage 1: Initial Engagement

Informal, face to face meetings were arranged with representatives of the practices to discuss the Authority's desire to conduct a thematic review.

Following this, the participating practices received a Terms of Reference ("ToR") letter, explaining the intended scope and purpose of the exercise, as well as the review phases detailed above.

Once the ToR had been agreed, further correspondence was issued by the Authority, outlining the specific processing it expected to be addressed. This helped direct the GP practices' efforts to collate relevant material based on the scope outlined.

All practices responded to the above, providing the requested material, at which point the Authority progressed to the Assessment phase.

Stage 2: Assessment

As part of the Assessment Phase, the Authority reviewed a range of document types, including:

- Policies and procedures relating to the access and use of Medicus.
- Data retention and disposal policies.
- Procedures for handling DSARs.
- Data Sharing Agreements.
- Privacy notices.

The documents were considered specifically with Medicus in mind and how internal processes would impact personal data held on the system. Where necessary, the Authority sought additional clarification from the practices by email or in discussion, the focus throughout being to identify what was working well and what could be strengthened.

All three practices demonstrated enthusiasm and a commitment to uphold their responsibilities under the Law

While the Authority identified positive measures, it did note certain areas where improvements were needed. These areas form the content for the next phase, Feedback.

Stage 3: Feedback

Following the assessment, the Authority provided each practice with a detailed written summary of its observations in the form of the 'Feedback phase'. Where appropriate, this feedback was accompanied by recommendations, designed to encourage the relevant GP practice to update their processes and governance, in accordance with the Authority's observations. Recommendations generally allowed for some flexibility by the practices, ensuring they could apply the findings effectively, utilising their own operational knowledge.

The practices were invited to respond to the Authority's feedback, confirming whether they accepted the recommendations and their anticipated completion dates. This period allowed any comments or concerns to be raised by the practices e.g. the practical implementation of certain recommendations. Where recommendations were accepted, the Authority would consider the proposed completion dates and determine whether the projected timeline was appropriate.

Finally, the Authority would respond to the practices acknowledging their acceptance and confirming the finalised deadlines for all agreed recommendations.

5. General findings

The findings set out below are presented in general terms and are not attributed to any single organisation.

5.1 Positive observations

The following positive findings were noted generally:

- All of the participating GP practices engaged positively and constructively with the review process, providing documentation and responding to queries in a timely manner.
- All demonstrated a clear understanding of their responsibilities under the Law and a genuine commitment to protecting the sensitive health information in their care.
- All demonstrated a clear willingness to improve their arrangements where needed.
- Whilst findings were made with respect to the organisation's governance (see below), the majority of documentation expected by the Authority was present.
- It was confirmed that a Data Protection Impact Assessment ("DPIA") had been conducted prior to the implementation of Medicus.

5.2 Areas requiring improvement

The review also identified a number of areas where improvements were needed, certain of which are listed below. Again, the following is generalised and not specific to any one organisation:

Finding 1: Governance documents pre-dating the new system

One observation made was that certain governance documents such as the data sharing agreement, as well as some internal policies, clearly pre-dated Medicus and had not been updated since its implementation. This meant certain documents used dated terminology or did not accurately reflect the processing performed by the new case management system.

Keeping governance documentation current is necessary to allow staff to adequately follow established processes and by extension ensure the GP practice itself complies with the requirements placed on it by the Law. Whenever a new system is introduced, steps should be taken to review all relevant governance and update accordingly.

Finding 2: Data Sharing Arrangements required strengthening

As three distinct controllers, utilising a system that allows for the sharing of personal data between the practices, the Law requires that a Data Sharing Agreement be in place to govern said sharing, detailing their respective roles, responsibilities and duties towards the individuals whose information they process.

Whilst a Data Sharing Agreement was in place, it pre-dated the introduction of Medicus and did not directly address the processing in question. A number of observations and suggested improvements were made, which the Authority flagged through feedback, recommending steps be collectively taken by the practices to either update or develop a wholly new document, specific to arrangement around Medicus.

Finding 3: Retention policies required clarification

The Authority identified instances where the defined retention period was either unclear or potentially excessive. This was communicated to the relevant practices and recommendations were issued to update the relevant documentation where appropriate taking into account, for example, guidance from relevant professional bodies. The Authority acknowledges that health records can be legitimately held for significant periods, however, this is not absolute and regular reviews of internal retention policies should be conducted to ensure personal data is held only as long as is necessary.

The Authority also noted the arrangement with the service provider who supports Medicus and potential conflicts between the retention periods of this third party and the GP practices themselves. Feedback was issued addressing this and requiring further clarification on the retention of patient data by both parties (controller and processor) should an individual leave the Medicus network entirely.

Finding 4: “Inactive” records lacked clear governance

When a patient leaves a practice, their records at that practice are marked as "inactive" within Medicus. This status allows the original practice to retain access to those records (with certain safeguards in place to limit access) in line with their established retention periods and, if necessary and lawful to do so, access the information (e.g. where providing certain types of care or responding to a DSAR).

The Authority found that, in some cases, governance lacked specific reference to “inactive” records and, as a result, staff may not have been fully informed about what this status means and any other related implications (i.e. when it should be accessed and by whom). As

per the next finding, this also risks overlooking inactive data when performing certain functions.

Finding 5: Data Subject Access Request procedures needed updating

Under the Law, individuals have the right to request a copy of the personal data processed by the controller (e.g. a GP practice). This request is typically called a Data Subject Access Request (DSAR). Following review of the related internal procedures, the Authority issued recommendations to update the relevant documentation accordingly. The required adjustments varied between each practice and ranged from inaccurate statutory deadlines (30 days stated as opposed to one calendar month) to not highlighting certain record types that may require additional steps to search/access e.g. archived or "inactive" records, as referenced above.

Up to date governance regarding data subject rights is an important feature of any organisation, especially one that regularly processes special category data. Staff should be fully versed on the DSAR procedure and the actions they must take when presented with a DSAR. This is typically communicated through internal documentation, as well as effective training inputs.

Finding 6: Records of Processing Activities required updating

In accordance with the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018, controllers are required to maintain a Record of Processing Activities ("RoPA"), detailing the personal data processed by the organisation alongside other information, such as the security measures taken in relation to the processing. An accurate RoPA is an important internal document, providing a current map of the personal data held and processes occurring across an organisation. This can have many applications, including providing a helpful blueprint for facilitating DSARs.

The Authority noted that, in some cases, these records had not been updated, following the implementation of Medicus, and so issued a recommendation to make any necessary amendments.

Finding 7: Privacy Notices required updating

Privacy or data processing notices form a core part of the transparency requirement under the Law, conveying important information to service users about their personal data and how the organisation is processing that information. Observations were made regarding practices' privacy notices and recommendations issued to ensure they effectively communicated all necessary information to individuals receiving medical care.

6. Outcomes

Following the review, all recommendations made by the Authority were accepted by the practices. The majority of commitments have now been completed and any remaining are currently being addressed.

Improvements include:

- Updates to policies addressing access to Medicus and staff roles.
- Updates to policies addressing patient transfer and inactive records.

- Updates to the retention and disposal of patient data.
- Updating or otherwise developing a Medicus-specific data sharing agreement between all surgeries utilising the system.

The scope of this review was deliberately focused on governance surrounding the Medicus system. It did not constitute a full audit of each practice's overall data protection compliance. The Authority, therefore, cautions other organisations not to interpret the completion of these recommendations as confirmation that any and all aspects of their compliance with the Law have been addressed. Organisations should endeavour to implement regular, structured reviews of their organisational and technical safeguard measures and promote an overall culture of dynamic improvement.

7. Key takeaways

The following key takeaways are offered as guidance. These can be applied to any organisation, regardless of size or sector:

Takeaway 1: When you adopt a new system, update your governance to match

Governance can often be seen as a 'one and done' matter. However, in addition to regular routine reviews, organisations should always make sure to consider relevant documents when introducing a new or improved technical measure, such as a case management system. While the changes may be relatively minor, small differences in how personal data is handled can lead to misunderstandings and failures in the process pipeline. Staff will rely on internal policies and procedures to perform their roles and, when presented with a non-routine request like a DSAR, may be unclear on the necessary steps to take, as well as where personal data may now be stored.

Up to date governance also demonstrates accountability, a key consideration of the Authority when reviewing an organisation's compliance.

Takeaway 2: Data Sharing Agreements must be clear and current

Similar to internal policies and procedures, Data Sharing Agreements are often overlooked once completed. These documents govern the sharing of personal data with other organisations and getting them right is vital as, once it is shared, control is lost over the personal data. Failure to manage these relationships properly can lead to misuse of service users' personal data and, by extension, a loss of trust in the organisation.

The Law lays out the information required in both controller/processor and controller/controller relationships. Organisations should consult the relevant sections of the Law, alongside the Authority's guidance to ensure their agreements are suitable and provide the necessary protections for personal data being shared.

Takeaway 3: Be mindful of retention periods

The Law's Storage Limitation principle requires that personal data is held only for as long as is necessary for the purpose for which it was collected. No personal data can be held indefinitely without ample justification.

Not only should retention periods be proportionate, they should be clearly detailed in internal documentation, with an established process for when the period expires. This reduces the risk of personal data being held longer than required or disposed of improperly. Due consideration is elevated where the information in question is Special Category Data such as health data.

The above extends to third party organisations processing personal data on behalf of the organisation and should be governed via the appropriate contractual clauses detailing when and under what circumstances the third party is expected to return/delete personal data provided by the controller.

Takeaway 4: Consider the uniqueness of your system and the data in it

Organisations sometimes make the error of addressing processes in a more general tone, without sufficient focus on the unique elements of their organisation and the systems they use.

It is important to look at systems and the ways they treat the personal information held, including the application of specific statuses that may alter how the information is handled and/or accessed. Where these are identified, organisational and technical measures should be implemented and reflected in internal documentation, sufficiently informing staff on the relevant nuances.

Takeaway 5: Make sure your DSAR procedures are accurate and complete

Individuals are becoming more confident in exercising their data subject rights, leading to an increase in DSARs across sectors. Healthcare providers are particularly susceptible to this increase as service users are understandably invested in information relating to their medical care.

Robust and clear DSAR procedures are, therefore, more important than ever in meeting this increased expectation from the public and complying with the requirements of the Law.

Small inaccuracies in details such as the designated disclosure deadline can lead to unnecessary instances of non-compliance and ultimately more headaches for the responsible organisation. It is, therefore, vital to keep these documents accurate and up to date, taking into account the introduction of new systems that may impact the DSAR procedure.

Takeaway 6: Proactive engagement with your regulator is a strength, not a weakness

In participating with this review, the GP practices demonstrated that proactive engagement with the regulator is to be embraced rather than avoided. It offers a valuable opportunity to identify and address gaps before they become problems.

Collaboration with the Authority through such reviews also demonstrates a high level of accountability, which is a key principle of the Law and is routinely factored into the Authority's regulatory enquiries. It also allows the organisation to take advantage of the expertise of Authority investigators.

As a result, commitments have been made that will place all three practices in a stronger position from a compliance perspective. This in turn improves the protections in place for the personal data of service users and increases trust in those organisations.

The Authority hopes that organisations uncertain about any aspect of their data protection arrangements feel encouraged to engage with the Authority to discuss. The Authority exists to support compliance, not simply to enforce it.

8. Conclusion

When implementing new technical measures within an organisation, controllers must consider their governance portfolio, taking steps to review and update where necessary. More than simply an administrative exercise, this prepares the organisation and its staff for ad-hoc processes, such as DSARs, which require a comprehensive and accurate understanding of internal procedures and the personal data processed.

Any internal reviews should extend to the sharing of personal data with other third parties, clarifying roles, responsibilities and other key information subject to that sharing.

It is important to note that the findings detailed in this report are not unique to the participants or the health sector. Any organisation that is using or intends to use a digital case management system, shared or otherwise, should consider whether their governance is fit for purpose.

In sharing the findings and key takeaways from this review, the Authority hopes that other organisations will take the opportunity to examine their own processes and consider what further steps they can take to safeguard sensitive personal data.

The Authority would like to thank the participants of this thematic review for their positive and constructive engagement. The improvements they have committed to will directly benefit the patients whose health data they are trusted to protect and will contribute to a stronger culture of data protection across the Bailiwick's health sector.

For further guidance on any of the topics covered in this report, please visit the ODPA's website at odpa.gg or contact the Authority using the details below.

Office of the Data Protection Authority
Block A | LeFebvre Court | LeFebvre Street | St Peter Port | Guernsey | GY1 2JP
T: +44 (0)1481 742074 | E: info@odpa.gg | W: odpa.gg

Published September 2026