CASE AUTH/3429/11/20 ***NO BREACH OF THE CODE***

MEMBER OF THE PUBLIC v SANOFI

Company responses to enquiries

This complaint arose from Case AUTH/3281/11/19 wherein the complainant, a member of the public, complained about various interactions he/she had had with Sanofi. The complainant provided a copy of an email he/she had sent to Sanofi which stated that when a member of Sanofi's staff called the complainant, the member of staff failed to say the call would be recorded. In addition, the complainant noted that normal record management systems would keep information for 6 years. Given that medical information needed to be held for longer as adverse reactions might occur, Sanofi's comment that 'For data security purposes, Sanofi has a 90-day automatic deletion policy on all e-mails sent to e-mail inboxes. This includes e-mails sent to individuals. This may explain why the e-mails from [a named Sanofi staff member] that you mentioned have not been provided.', in the complainant's view, indicated a clear breach of GDPR (General Data Privacy Regulation) as Sanofi was firstly implying that Sanofi's email system was insecure and secondly Sanofi was allegedly destroying emails which might be relevant for future reference. The complainant asked why this 90-day retention period was not mentioned to anyone emailing Sanofi and why it was missing from Sanofi's Privacy Policy.

The detailed response from Sanofi is given below.

The Panel noted that Sanofi's medical information function was outsourced to an agency. It was an established principle that companies were responsible for the acts and omissions of their agencies that came within the scope of the Code. The Panel also noted that the complainant bore the burden of proof and had to establish his/her case on the balance of probabilities.

The Panel noted Sanofi's submission that at the beginning of each inbound medical information call, callers were advised 'calls are recorded for quality and training purposes'. In cases where the call could not be taken immediately, it might be necessary to return the call which Sanofi explained would represent a continuation of that call. Sanofi stated that the message regarding recording of calls was not repeated in the context of return calls. The call which was the subject of this complaint was such a return call and, according to Sanofi, contained sensitive personal data. The Panel noted Sanofi's response that following this complaint Sanofi had now revised the enquiry handling process to remind recipients of outgoing calls that such calls were being recorded.

The Panel did not have a copy of the privacy policy in place at the time the call was made to the complainant but noted that the privacy policy provided by Sanofi, last updated December 2019, stated:

'Data that we collect automatically, for instance recordings of telephone calls when you call SANOFI or we call you (you will always be notified in advance when we are intending to record a telephone call).'

Management of personal data was an important issue. The Panel noted that Sanofi had not argued that the matter was not within the scope of the Code. The Panel noted the scope of the Code as set out at Clause 1.1. Whilst the Code did not explicitly refer to GDPR, Clause 1.11 stated that pharmaceutical companies must comply with all applicable codes, laws and regulations to which they are subject. In the Panel's view, this meant codes, laws and regulations that related to matters that fell within the scope of the ABPI Code. Whether matters in relation to GDPR fell within the scope of the Code would be decided on a case-by-case basis. The Panel noted that the complaint concerned GDPR in relation to medical information interactions. The Panel noted from the evidence before it that there did not appear to have been any formal finding by any judicial authority or appropriate body formally charged with determining matters in relation to GDPR that Sanofi had not complied with the relevant laws and regulations in relation to the telephone call in question. The Panel therefore ruled no breach of the Code.

The Panel noted the complainant's allegation that a 90-day automatic deletion policy on all emails sent to email inboxes was inadequate for medical information as adverse reactions might occur.

The Panel noted that whether allegations about an email retention policy came within the scope of the Code would be decided on a case-by-case basis and noted, again, that Sanofi had not commented on this point. The Panel noted that it appeared that the medical information emails in question were retained for 30 years rather than deleted after the 90-day period referred to by the complainant. The Panel noted, however, that the letter dated 16 December 2019 from Sanofi to the complainant referred to a 90-day automatic deletion policy on all emails sent to email inboxes including emails to individuals. The Panel thought it odd that Sanofi had not referred to the 30 year policy in relation to medical information in this letter. The Panel noted that the complainant's allegation related specifically to medical information emails particularly in relation to adverse events and, in this regard, considered that the complainant had not established that such emails were insecure or automatically deleted as alleged. No breach of the Code was ruled.

The Panel noted from the evidence before it that there did not appear to have been any formal finding by any judicial authority or appropriate body formally charged with determining matters in relation to GDPR that Sanofi had not complied with the relevant laws and regulations in relation to its data retention policy. The Panel therefore ruled no breach of the Code. Nor had the complainant established that Sanofi's data retention policy was such that adverse events were not appropriately captured and managed. No breach of the Code was ruled.

Although the Panel had concerns in relation to the letter dated 16 December 2019 from Sanofi to the complainant, these were not matters raised by the complainant. In the Panel's view, the cited clause was not relevant in relation to the allegations raised and the Panel therefore ruled no breach of the Code.

The Panel noted Sanofi's submission that a review of the emails held by Sanofi relating to the complainant had identified some references to off-line discussions which, according to Sanofi, was not unusual if there were complex situations which would benefit from more detailed verbal discussion between two or more Sanofi personnel. No cases had been identified where Sanofi colleagues had sought to 'avoid being captured by GDPR' by advising talking to each other rather than corresponding by email. The Panel noted that Sanofi had not commented on whether this matter came within the scope of the Code. The Panel noted that the complainant bore the burden of proof and considered that the complainant had not established that Sanofi employees attempted to avoid being captured by GDPR in the manner alleged. No breach of the Code was ruled.

This complaint arose from Case AUTH/3281/11/19 wherein the complainant, a member of the public, complained about various interactions he/she had had with Sanofi. During the Code of Practice Panel's consideration of Case AUTH/3281/11/19, it did not have before it the complainant's later additional allegations nor Sanofi's response to these additional allegations and thus made no ruling on these matters in that case. These additional matters were referred to the Panel for consideration as the present case, Case AUTH/3249/11/20.

The additional allegations comprised an email dated 16 December 2019 from the complainant to a named individual at Sanofi which was copied to the PMCPA. In support, the complainant also provided a copy of a letter sent by email from Sanofi to the complainant also dated 16 December 2019.

COMPLAINT

The complainant provided a copy of an email he/she had sent to Sanofi and stated that he/she had copied this email to the PMCPA as Sanofi's actions were relevant to an ongoing complaint about Sanofi's conduct and this unethical behaviour was against the ABPI Code. In the email, the complainant stated that when the Sanofi member of staff called the complainant he/she failed to say the call would be recorded. In addition, the complainant noted that normal record management systems would keep information for 6 years. Given that medical information needed to be held for longer as adverse reactions might occur, Sanofi's comment 'For data security purposes, Sanofi has a 90-day automatic deletion policy on all e-mails sent to e-mail inboxes. This includes e-mails sent to individuals. This may explain why the e-mails from [a named staff member] that you mentioned have not been provided.', in the complainant's view, indicated a clear breach of GDPR as Sanofi was implying that (1) Sanofi's email system was insecure and (2) Sanofi was destroying emails which might be relevant for future reference. The complainant asked why this 90-day retention period was not mentioned to anyone emailing Sanofi and why it was this missing from Sanofi's Privacy Policy. The complainant noted that Sanofi had failed to answer why colleagues wrote to call each other to talk about the complainant to avoid being captured by GDPR which was both unethical and illegal.

When writing to Sanofi, the Authority asked it to consider the requirements of Clauses 1.11, 7.2 and 9.1 of the Code.

RESPONSE

Sanofi submitted that on 23 October 2019, the complainant made a formal subject access request which was acknowledged by Sanofi on 24 October 2019. Meanwhile, on 29 October

2019 the complainant forwarded to Sanofi an article from The Times about the use of 0845 numbers.

On 4 November 2019, Sanofi and the complainant exchanged emails clarifying the scope of the subject access request, and an update on the data collection process was sent by Sanofi to the complainant by letter dated 22 November 2019.

On 4 December 2019, a substantive response to the subject access request was sent to the complainant by encrypted email on 4 December 2019, however, the complainant was unable to open the files. On 9 December 2019, the complainant therefore agreed to receive the response via a password protected internet platform (Dropbox) and a link was sent. The complainant criticised Sanofi's response to the subject access request on the basis that certain correspondence was missing. A further document was subsequently identified by Sanofi (it seemed likely to have been missed initially as it was an attachment to another email) and was provided to the complainant by Dropbox in December 2019 with a letter responding to his/her concerns.

Following receipt of Sanofi's response to the subject access request, the complainant sent a further email also on 16 December 2019, copied to PMCPA, stating that Sanofi's actions were 'relevant to an ongoing complaint about Sanofi's conduct' and listed examples of what he/she described as 'unethical behaviour'. This was the email attached to the PMCPA's letter of January 2020 and the matters raised by the complainant are addressed below.

New points of complaint raised by the complainant with Sanofi's responses

1 *'When [a named member of staff] called me on my mobile [he/she] failed to say that the call would be recorded'*

The email from the complainant dated 16 December 2019, did not explain the basis for the complaint in respect of the above matter. However, the complainant's earlier email of 11 December 2019, indicated that he/she was alleging a breach of GDPR.

At the time of the complaint, Sanofi's medical information function was outsourced to a third party.

At the beginning of each inbound call, callers were advised 'calls are recorded for quality and training purposes'; a transcript of the privacy message provided to callers at the beginning of each inbound call was provided. In cases where the call could not be taken immediately, it might be necessary to return the call. Outbound calls were made only in order to return an inbound call and represent a continuation of that call. The message regarding recording of calls was not repeated in the context of return calls. The call which was the subject of this complaint was such a return call; it included sensitive personal data (information provided by the complainant in relation to his/her health).

Sanofi did not believe this was a breach of the GDPR by Sanofi or the agency as follows:

- The purpose of the message regarding call recording was to ensure that callers were aware that calls would be recorded, so that if they objected, they could decide not to proceed with the call. Guidance issued by the Information Commissioner (the competent authority in the UK for the purposes of GDPR) addressed the 'right to be

informed' under Articles 13 and 14 of the GDPR (and the Data Protection Act 2018) and confirmed that there was no obligation to repeat information which had already been provided.

- Return calls were made shortly after an inbound call and formed part of the same discussion; clearly therefore the information provided at the start of an incoming call applied equally to the return call.

- In any event, the complainant clearly recalled the information provided to him/her when he/she called Sanofi medical information, which included that 'calls are recorded for quality and training purposes', as evidenced by the emails of September and October 2019, which referred to 'long statements on GDPR' given on inbound calls.

In summary, Sanofi did not believe the matter complained of by the complainant demonstrated a breach of GDPR and there was accordingly no breach of Clause 1.11 of the Code. Nevertheless, while there were disadvantages in repeating the privacy information provided to members of the public when they called Sanofi's medical information service, in the context of a return call (in particular, duplication of detailed information), following this complaint Sanofi had revised the enquiry handling process to remind recipients of outgoing calls that the calls were being recorded.

For completeness, in circumstances where Sanofi accepted (a) that the privacy message provided in the context of all inbound calls was not repeated where those calls were returned and (b) that the call which was the subject of the complaint contained sensitive personal data, Sanofi did not believe it was necessary to provide a copy of the recording or a transcript. Unnecessary disclosure of personal data might itself constitute a breach of GDPR.

2 *'In addition normal records management systems would keep information for 6 years. Given that medical information needs to be longer given ADRs may occur your comment "For data security purposes, Sanofi has a 90-day automatic deletion policy on all e-mails sent to e-mail inboxes. This includes e-mails sent to individuals. This may explain why the e-mails from [a named member of staff] that you mentioned have not been provided." indicates a clear breach of GDPR as you are implying that 1) Your email system is insecure and 2) You are destroying emails which may be relevant for future reference.*

Why is this 90-day retention period not mentioned to anyone emailing you and is missing from your Privacy Policy?.'

The complainant's assertion that 'normal records management systems would keep information for 6 years' was not referenced and Sanofi did not believe that there was any legal or other obligation to retain all information provided to the company for such a period.

Under GDPR (and the Data Protection Act 2018) personal data must not be retained for longer than is necessary for its lawful purpose. In this context, Sanofi's processes relating to email management might be summarized as follows:

'• Any Adverse Events or suspected Adverse Events within any incoming emails from any source are reported to our Pharmacovigilance Team. These events and e-mails

are then held in our Pharmacovigilance Database in accordance with regulatory requirements.

- Any incoming e-mails containing a specific Medical Information Enquiry are forwarded to our Medical Information Team to answer and are stored in our Medical Information Database. Sanofi policy is to store the incoming Medical Information Enquiry and the Medical Information Response for a period of 30 years.

- Other e-mail inboxes are subject to a 90-day retention policy for data management and efficiency purposes within Sanofi, consistent with the information provided in Sanofi's Privacy Policy which is published on our website www.sanofi.co.uk which states "SANOFI will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, as outlined in this Policy". This arrangement reflects the requirement under GDPR (and the 2018 Act) that personal data may be retained for no longer than is necessary for the purposes for which it was processed - the shortest time possible. (The 90-day retention period does not apply to e-mails and other documents stored in the Pharmacovigilance and Medical Information Databases.).'

For completeness, Sanofi submitted that its retention policy did not indicate that its systems were insecure (the measures put in place to protect personal data were described in the Privacy Policy) and storage of personal data simply because it might potentially be relevant for future reference was contrary to the requirements of GDPR.

There was no basis for a finding of breach of GDPR or Clause 1.11 of the Code as a result of such matters.

3 'I note that you have failed to answer why your colleagues wrote to call each other to talk to me to avoid being captured by GDPR which is both unethical but illegal?'

A review of the emails held by Sanofi relating to the complainant had identified some references to off-line discussions; these were provided. This was not unusual if there were complex situations which would benefit from more detailed verbal discussion between two or more Sanofi personnel. No cases had been identified where Sanofi colleagues had sought to 'avoid being captured by GDPR' by advising talking to each other rather than corresponding by email. Furthermore, GDPR required that personal data that were held or processed were limited to those that were necessary for the defined purpose; there was no obligation under GDPR to generate additional documents referencing personal data in order to create a record and to do so would potentially conflict with the requirement not to hold more personal data than was required.

Sanofi submitted that there was no basis for a finding of breach of GDPR, breach of Clause 1.11 of the Code or unethical conduct by it as a result of such matters.

Overall conclusion

Following investigation of the multiple points raised within this case, Sanofi had reviewed the available evidence and had not identified any information which indicated breaches of the Code clauses which it was asked to consider.

The latest complaint from this complainant related to alleged breaches of GDPR. The PMCPA supervised the Code, which focussed on the promotion of medicinal products and related activities. It was not the competent authority for the purposes of data privacy and Sanofi respectfully suggested that PMCPA might not properly make adverse findings in relation to GDPR matters.

Despite the caveat set out above, Sanofi had investigated the additional matters raised by the complainant in the context of this further complaint and believed the arrangements for Sanofi's medical information service (including those aspects outsourced to an agency) were compliant with the requirements of the GDPR. No other basis for a possible breach of Clause 1.11 had been alleged.

Clause 7.2 of the Code dealt with information claims and comparisons in relation to medicines. Sanofi did not believe this clause was relevant to the current complaint and the matters set out above.

Clause 9.1 of the Code dealt with the maintenance of high standards. In circumstances where no breach of any other clause of the Code was evidenced by the matters raised by the complainant in this further complaint and where Sanofi had co-operated with the complainant to respond to his enquiries and correspondence, Sanofi submitted that there was no basis for any finding of breach of Clause 9.1.

PANEL RULING

The Panel noted the complainant's allegation that the failure of Sanofi's medical information department to state that a telephone call to him/her was recorded, was a breach of the General Data Protection Regulations (GDPR). The Panel noted that Sanofi's medical information function was outsourced to an agency. It was an established principle that companies were responsible for the acts and omissions of their agencies that came within the scope of the Code. The Panel also noted that the complainant bore the burden of proof and had to establish his/her case on the balance of probabilities.

The Panel noted Sanofi's submission that at the beginning of each inbound medical information call, callers were advised 'calls are recorded for quality and training purposes'. In cases where the call could not be taken immediately, it might be necessary to return the call which Sanofi explained would represent a continuation of that call. Sanofi stated that the message regarding recording of calls was not repeated in the context of return calls. The call which was the subject of this complaint was such a return call and, according to Sanofi, contained sensitive personal data. The Panel noted that the letter from Sanofi to the complainant dated 16 December stated that 'all outbound calls from Medical Information are **now** routinely started with a privacy notice. The team have been instructed to state that the calls are being recorded' (emphasis added). The letter also stated that when a customer was called back from a mobile these calls were not recorded and the patient was made aware of this. The Panel noted that Sanofi's response stated that in the context of a return call (in particular, duplication of detailed information), following this complaint Sanofi had now revised the enquiry handling process to remind recipients of outgoing calls that such calls were being recorded.

The Panel did not have a copy of the privacy policy in place at the time the call was made to the complainant but noted that the privacy policy provided by Sanofi, last updated December 2019 stated:

> **'Data that we collect automatically**, for instance recordings of telephone calls when you call SANOFI or we call you (you will always be notified in advance when we are intending to record a telephone call).'

Management of personal data was an important issue. The Panel noted that Sanofi had not argued that the matter was not within the scope of the Code. The Panel noted the scope of the Code as set out at Clause 1.1. Whilst the Code did not explicitly refer to GDPR Clause 1.11 stated that pharmaceutical companies must comply with all applicable Codes, laws and regulations to which they are subject. In the Panel's view this meant codes, laws and regulations that related to matters that fell within the scope of the APBI Code. Whether matters in relation to GDPR fell within the scope of the Code would be decided on a case-by-case basis. The Panel noted that the complaint concerned GDPR in relation to medical information interactions. The Panel noted from the evidence before it that there did not appear to have been any formal finding by any judicial authority or appropriate body formally charged with determining matters in relation to GDPR that Sanofi had not complied with the relevant laws and regulations in relation to the telephone call in question. The Panel therefore ruled no breach of Clause 1.11 of the Code.

The Panel noted the complainant's allegation that a 90-day automatic deletion policy on all emails sent to email inboxes was inadequate for medical information as adverse reactions might occur. In this regard, the Panel noted Sanofi's response that it did not believe that there was any legal or other obligation to retain all information provided to the company for a 6 year period as stated by the complainant and that its policy was to store the incoming Medical Information Enquiry and the Medical Information Response for a period of 30 years. The Panel noted Sanofi's submission that any adverse events or suspected adverse events within any incoming emails from any source were reported to its pharmacovigilance team. These events and emails were then held in its Pharmacovigilance Database in accordance with regulatory requirements. Other email inboxes were subject to a 90-day retention policy for data management and efficiency purposes within Sanofi, consistent with the information provided in Sanofi's privacy policy which was published on its website and stated 'SANOFI will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, as outlined in this Policy'. Sanofi stated that this arrangement reflected the requirement under GDPR (and the 2018 Act) that personal data may be retained for no longer than is necessary for the purposes for which it was processed – the shortest time possible. The Panel noted Sanofi's submission that the 90-day retention period did not apply to emails and other documents stored in the Pharmacovigilance and Medical Information databases.

The Panel noted that whether allegations about an email retention policy came within the scope of the Code would be decided on a case-by-case basis and noted, again, that Sanofi had not commented on this point. The Panel noted that it appeared that the medical information emails in question were retained for 30 years rather than deleted after the 90-day period referred to by the complainant. The Panel noted, however, that the letter dated 16 December 2019 from Sanofi to the complainant referred to a 90-day automatic deletion policy on all emails sent to email inboxes including emails to individuals. The Panel thought it odd that Sanofi had not referred to the 30 year policy in relation to medical information in this letter. The Panel noted that the complainant's allegation related specifically to medical information emails particularly in relation to adverse events and, in this regard, considered that the complainant had not established that such emails were insecure or automatically deleted as alleged. No breach of Clause 9.1 was ruled.

The Panel noted from the evidence before it that there did not appear to have been any formal finding by any judicial authority or appropriate body formally charged with determining matters in relation to GDPR that Sanofi had not complied with the relevant laws and regulations in relation to its data retention policy. The Panel therefore ruled no breach of Clause 1.11 of the Code. Nor had the complainant established that Sanofi's data retention policy was such that adverse events were not appropriately captured and managed. No breach of Clause 9.1 was ruled.

Although the Panel had concerns in relation to the letter dated 16 December 2019 from Sanofi to the complainant, these were not matters raised by the complainant. In the Panel's view, Clause 7.2 was not relevant in relation to the allegations raised and the Panel therefore ruled no breach of Clause 7.2.

The Panel noted Sanofi's submission that a review of the emails held by Sanofi relating to the complainant had identified some references to off-line discussions which, according to Sanofi, was not unusual if there were complex situations which would benefit from more detailed verbal discussion between two or more Sanofi personnel. No cases had been identified where Sanofi colleagues had sought to 'avoid being captured by GDPR' by advising talking to each other rather than corresponding by email. The Panel noted that Sanofi had not commented on whether this matter came within the scope of the Code. The Panel noted that the complainant bore the burden of proof and considered that the complainant had not established that Sanofi employees attempted to avoid being captured by GDPR in the manner alleged. No breach of Clause 9.1 was ruled.

Complaint received **16 December 2019**

Case completed **6 August 2021**