[doc. web no. 9861289]

Injunction against the Local Health Authority n.5 Polesana - 26 January 2023

Register of measures

no. 26 of 26 January 2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, components and the cons. Fabio Mattei, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE, “General Data Protection Regulation” (hereinafter the “Regulation”);

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data", containing provisions for the adaptation of national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/EC (hereinafter the "Code");

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

Given the documentation in the deeds;

Given the observations made by the general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker Prof. Pasquale Stanzione;

WHEREAS

1. The notification of violation and the preliminary investigation

With communication of the XX, integrated with a subsequent note of the XX, the Local Health Authority n.5 Polesana, located

in Rovigo, Viale Tre Martiri 89, postal code 45100 – Fiscal Code 01013470297, PEC: protocol.aulss5@pecveneto.it. (hereinafter "Company") has notified, pursuant to art. 33 of the Regulation, a violation of personal data concerning a communication of data relating to health to an unauthorized third party.

In particular, the Company, with regard to this event, declared that, "the medical record was delivered on the XX date. With pec of the XX the patient communicated that the copy of the medical record delivered contained documentation not attributable to himself. Only later (on the XX date), upon return of a copy of the medical record, was it possible to verify that the health documentation attributable to a different subject reported the name of the third party".

The Company also specified that the verification carried out by the Medical Directorate of the Rovigo Hospital "has revealed the presence of the following documentation belonging to a third party: no. 30 pages of medical records of which n. 3 pages referable to the clinical diary, n. 15 attributable to the therapies prescribed and performed and n. 12 pages attributable to the history of medical diaries and prescribed and administered therapies (comparable in terms of content to the clinical diary and prescribed and administered therapies, with specific date and time of compilation by the healthcare personnel)".

What technical and organizational measures adopted (or whose adoption is proposed) to prevent similar future violations, in addition to the request for the return of all the documentation delivered, have been indicated by the Company: "Update of the internal procedure for issuing medical records , accompanied by a checklist to be compiled on a sample basis to verify the integrity of the individual medical records. Request to anyone who has a role in the process of preparing the medical record to deliver to the Director of the U.O.C. the medical record of which a copy has been requested before reproduction so that the same can further check its completeness and correct composition. In addition, a specific training course will be provided for all those involved in the collation and completion, handling and reproduction of medical records to follow".

On the basis of what was represented by the data controller in the deed of notification of the violation as well as the subsequent assessments, the Office, with deed of the XX (prot. n. XX), notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions referred to in article 58, par. 2, of the Regulation.

In particular, the Office, in the aforesaid deed, found that the Company - by inserting a patient's health documentation in a medical record relating to a different patient and delivered to the latter - communicated personal data and related to health in the absence of a suitable legal prerequisite in violation of the basic principles of treatment pursuant to articles 5 and 9 of the

Regulation and the safety obligations pursuant to art. 32 of the same Regulation.

In relation to this, the Office has also invited this data controller to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of Law No. 689 of 11/24/1981).

With note of the XX (prot. n. XX), the Company produced a defense brief, in which, in addition to what is represented in the deed of notification of violation, it highlighted, among other things, that:

- "the facts of the matter took place inside the Trecenta Hospital, at the time (and still now) identified as a Covid Hospital for the Province of Rovigo, with a number of 72 beds intended for the treatment of patients which required a high assistance and organizational commitment. Given the type of hospitalized patients, in order to preserve the safety of the operators (both those required to compile the medical records, and those who would then have to manage their conservation and any copy extraction upon request), the section of file compiled within the ward and, therefore, in close contact with the patients, was kept, for a certain period of time, in a separate space from the one in which the remaining part of the file was compiled and kept before sending to the Medical Directorate for subsequent filing. Only at a later time were the two sections of the medical record assembled and merged into the patient's hospital medical record. This particular type of "path" of the medical record may have influenced the commission of the human/material error which then occurred";
- "Due to the evolution of the pandemic emergency, this extraordinary operating practice of separate management of the medical record has been superseded as it was no longer deemed necessary and in any case the procedure for the overall management of the medical record (...) has been revised";
- "(...) following the report, the Medical Reports Collection Office contacted the patient to have him return the entire medical record received, including the documentation relating to the different patient; and on the XX date, the whistleblower's wife, provided with a proxy, proceeded to return the entire package of health documentation received and to collect her husband's medical records. (...) The whistleblower, in addition to having returned copies of the entire documentation received, confirmed by telephone to this Company that he had not extracted further copies and that he would observe the utmost confidentiality with regard to any information he might learn";
- "The violation concerned only one interested party (a patient of the undersigned Company), involved data of a common nature and data of a particular nature (as they relate to health) and ceased its effects as early as the date of the preliminary

notification, forwarded to this Authority on the same date as that on which the whistleblower returned the documentation";

- “This company has been adopting measures for some time to avoid events such as the one involved in the violation: in particular, procedures have been adopted and training courses have been organized regarding the correct compilation and management of medical records. The effectiveness of these measures is confirmed by the fact that the personal data breach in question is the first to have occurred with regard to the release of copies of medical records and is also attributable to a mere human error, which moreover occurred in one state of pandemic emergency with inevitable repercussions also on the company organisation”;

- "The operating procedure concerning the procedures for verifying the completeness of the medical records was updated on the XX date - a few days after the detection of the event - also in order to provide for different levels of control of the records, so as to further limit the likelihood that events like the one in question will recur. The aforementioned procedure provides that the verification of the completeness of the medical record is entrusted to the cross-check of the Director/Manager and the Nursing Coordinator of the operating unit where the patient is hospitalized, who will have to verify the presence of the various documents within the file clinic by completing and signing the relative check-list, each for the part of its competence. In the event of failure to complete the aforementioned check-list, the medical record cannot be taken into custody by the Medical Record Archive. Lastly, a subsequent sample check was envisaged on the conformity of the medical records deposited in the Medical Records Archive";

- "During the months of XX, the Company held, as part of its training program, a specific event repeated on four different dates, concerning "Clinical safety to protect liability: notions of clinical risk and forensic medicine" , which also dealt with the issue of managing health records and clinical information".

Lastly, the Company, for the reasons set out above, requested the filing of the proceeding or, alternatively, "the application of the minimum penalty deemed necessary".

2. Outcome of the preliminary investigation

Having taken note of what was represented and documented during the preliminary investigation procedure by the Company, with the violation notification deeds and, subsequently, with the defense brief produced following the deed notified by the Authority itself, pursuant to art. 166, it is noted that:

1. the processing of personal data must take place in compliance with the applicable legislation on the protection of personal

data and, in particular, with the provisions of the Regulation and of the Code. With particular reference to the question raised, it should be noted that "data relating to health" are classified as "personal data relating to the physical or mental health of a natural person, including the provision of health care, which reveal information relating to his state of health" (art. 4, par. 1, n. 15 of the Regulation) and that, therefore, the information object of the notification constitutes data relating to health;

2. the regulation on the protection of personal data provides - in the health sector - that information on the state of health can only be communicated to the interested party and can be communicated to third parties only on the basis of a suitable legal prerequisite or with a written authorization from the interested party (art. 9 of the Regulation and art. 84 of the Code in conjunction with art. 22, paragraph 11, Legislative Decree no. 101 of 10 August 2018);

3. the data controller is, in any case, required to respect the principles of data protection, including that of "integrity and confidentiality", according to which personal data must be "processed in such a way as to guarantee 'adequate security (...), including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage" (Article 5, paragraph 1, letter f) of the Regulation );

4. the adequacy of these measures must be assessed by the data controller with respect to the nature of the data, the object, the purposes of the processing and the risk for the fundamental rights and freedoms of the data subjects, taking into account the risks deriving from destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed (Article 32, paragraphs 1 and 2 of the Regulation).

5. the Company confirmed, in the defense brief, the communication of the data relating to the health of no. 1 patient interested in another patient not authorized to receive them and also highlighted that it was an isolated case in the release of a copy of the medical record, which occurred due to a human error. Furthermore, she reiterated that, as soon as she became aware of the incident from this third recipient, she asked the latter, and obtained, the return of the entire medical record received, as well as confirmation of the maximum confidentiality with regard to any information learned and that in the days immediately following the detection of the event, it proceeded to update the operating procedure relating to the procedures for verifying the completeness of the medical records and organized training events for personnel on the subject of medical documentation management.

3. Conclusions

In the light of the assessments referred to above, taking into account the statements made by the data controller during the

preliminary investigation □ the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code (“False statements to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor”)□ it is represented that the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with the deed of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the preliminary assessments of the Office are confirmed and the illegality of the processing of personal data carried out by the Company is ascertained for having put in place - by inserting a patient's health documentation in a medical record relating to a different patient and a the latter delivered - a communication of personal and health-related data in the absence of a suitable legal prerequisite in violation of the basic principles of treatment pursuant to articles 5, par. 1, lit. a) and f) and 9 of the Regulation and the safety obligations pursuant to art. 32 of the same Regulation.

The violation of the aforementioned provisions makes it applicable, pursuant to art. 58, par. 2, lit. i), of the Regulation, the administrative sanction provided for by art. 83, par. 4, lit. a) and par. 5, letter. a) of the same Regulation, as also referred to by art. 166, paragraph 1 and 2, of the Code.

In this context, considering, in any case, that the Company has declared that, as soon as it became aware of the incident from the unauthorized third party, it asked the latter, and obtained, the return of the entire medical record received in addition confirmation of the maximum confidentiality regarding any information learned and which, in the days immediately following the detection of the event, proceeded to update the operating procedure relating to the procedures for verifying the completeness of the medical record and organized training events for personnel on the subject management of medical documentation, the conditions for the adoption of measures, of a prescriptive or inhibitory type, pursuant to art. 58, par. 2 of the Regulation.

4. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code).

The violation of the articles 5, par. 1, lit. a) and f), 9 and 32 of the Regulation caused by the conduct put in place by the Company, is subject to the application of the administrative fine pursuant to art. 83, par. 4, lit. a) and par. 5, letter. a) of the Regulation and 166, paragraphs 1 and 2, of the Code.

Consider that the Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures

referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 83, par. 2, of the Regulation in relation to which it is observed that:

- the communication made by the Company concerned data relating to the health of a single patient (Article 83, paragraph 2, letter a) and g) of the Regulation);
- it was an isolated case and with respect to the matter no malicious behavior on the part of the data controller emerges since the violation occurred due to an error by the operator (see defense brief, of the XX - prot. n. XX: "the violation of the personal data in question turns out to be the first to have occurred with regard to the release of copies of medical records and is also attributable to a mere human error, which moreover occurred in a state of pandemic emergency with inevitable repercussions also on the company organization " ) (Article 83, paragraph 2, letter b) of the Regulation);
- against the same Health Authority, no measures concerning pertinent violations have been previously adopted (Article 83, paragraph 2, letter e) of the Regulation);
- the Company has behaved collaboratively with the Authority (Article 83, paragraph 2, letter f) of the Regulation);
- the Company promptly took steps to adopt measures aimed at preventing the recurrence of the incident (Article 83, paragraph 2, letter f) of the Regulation);
- the Healthcare Authority, having become aware of the violation following the communication by the recipient of the documentation, who was not authorized to receive it, promptly and independently notified this violation to the Authority pursuant to art. 33 of the Regulation (art. 83, paragraph 2, letter h) of the Regulation);
- the conduct has also matured as part of the management changes in the procedures for the differentiated compilation of the medical record, as described above, determined by the specific safety needs of the operators, due to the emergency context deriving from the Covid-19 epidemic (art. 83, paragraph 2, letter k) of the Regulation).

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, letter. a) of the Regulations, to the extent of 5,000.00 (five thousand) euros for the violation of articles 5, par. 1, lit. f), 9 and 32 of the Regulation as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that, due to the nature of the data being processed unlawfully, the ancillary sanction of publication on the website of the Guarantor of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTOR

declares the illegality of the processing of personal data carried out by the ULSS n.5 Polesana, located in Rovigo, Viale Tre Martiri 89, postal code 45100 – Fiscal Code 01013470297 for the violation of the articles 5, par. 1, lit. f), 9 and 32 of the Regulation in the terms referred to in the justification;

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the aforementioned Company, to pay the sum of 5,000.00 (five thousand) euros as an administrative fine for the violation indicated in this provision; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed;

ENJOYS

to the aforementioned Health Authority, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of Euro 5,000.00 (five thousand) according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law n. 689/1981.

HAS

pursuant to art. 166, paragraph 7, of the Code, the entire publication of this provision on the website of the Guarantor and believes that the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external

relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the appellant resides abroad.

Rome, 26 January 2023

PRESIDENT

Station

THE SPEAKER

Station

THE SECRETARY GENERAL

Matthew