THE
NATIONAL LAW REVIEW

France Issues New Rules for the Accreditation of Health Data Hosting Services Providers

SQUIRE PATTON BOGGS
Article By
Stéphanie Faber
Squire Patton Boggs (US) LLP
SECURITY & PRIVACY // BYTES

- Communications, Media & Internet
- Health Law & Managed Care
- Global

- France

Thursday, May 3, 2018

As some companies may have experienced already, the French Public Health Code (Article L.1111-8) requires that services providers hosting certain types of health/medical data (in French "*hébergeurs de données de santé*" or "HDS") be accredited for this activity.

The accreditation procedure is changing, effective 1 April 2018, from an authorisation procedure to a certification

Type of processing activities and of data covered by the regulation

The obligation for an HDS to be accredited stems from the tentative creation of an online-shared medical record for each patient, and for which additional security was to be ensured by such accreditation. The obligation has evolved to apply to more extensive sets of data than just the medical file.

This obligation currently applies to "*any person hosting personal* ***health data collected on the occasion of prevention, diagnosis, care or social and medico-social follow-up activities***" on behalf of third parties that are either,

- *“individuals or legal persons at the origin of the production or collection of such data”* (the implementing decree referred to below, specifies that these persons are “data controllers”); or

- *“the patient himself.”*

The accreditation is not required for data controllers (e.g., healthcare professionals, hospitals…) who host their own data.

The HDS’ personnel are bound by professional secrecy obligations. The HDS cannot use the data for any other purpose nor sell the data, even with the data subject’s consent. It has to return the data at the end of the services. The HDS does not need to host the data in France.

Hosting of such data previously required the patient’s consent. Since 2016, this opt in requirement has been replaced by a right to opt out. The patient or “data subject” has to be informed and has the right to object to the host moving.

The authorisation procedure

Until 1 April 2018, the HDS had to be authorised by the French ministry of health following an application with ASIP-Santé (governmental agency for health). Authorisation is granted for 3 years and can be renewed.

The requirements were both financial and technical, to offer adequate security for such data. The hosting services provider must have a doctor amongst its staff, who will be in charge of access requests by patients. The application for approval has to contain, amongst other information, the standard services agreement of the HDS. There are many constrains relating to the confidentiality, security and access to this data.

Certification process starting 1 April 2018

After 1 April 2018, the HDS must be certified by an accreditation body authorised, in France by the COFRAC and, in the EU by the national equivalent of the COFRAC. The certification process and other regulatory requirements have been enacted by a Decree of 28 February 2018 (the “Decree”) which created, effective 1 April 2018, new articles R1111-8-8 to R1111-11 of the Public Health code.

Relevant services requiring certification

The Decree has established a detailed list of the activities that fall under the definition of HDS and require certification:

1. Supply and maintenance in operational condition of physical sites to host the physical infrastructure of the IT system used for the processing of health data;

2. Supply and maintenance in operational condition of the physical infrastructure of the IT system used for the processing of health data;

3. Supply and maintenance in operational condition of the virtual infrastructure of

the IT system used for the processing of health data;

4. Supply and maintenance in operational condition of the platform for hosting applications of the IT system;

5. Administration and operation of the IT system containing the health data;

6. Backup of health data.

There are two sets of certifications depending on the activity: certification for physical infrastructure hosting services ("*hébergeur infractructure physique*") for one or several of activities in 1 and 2, above, and certification for outsourcing hosting services ("*hébergeur infogéreur*") for one or several of activities in 3 to 6, above. A company may require either or both depending on its services.

As a result of this list, companies that may not have needed to obtain an authorisation in the past (because they were not hosting the data per say, but managing their application in IT system of the HDS), will now be required to obtain the relevant certification.

- **Specifications and procedure**

The specifications for certification are based on: ISO/IEC 27001 ; ISO/IEC 20000 ; ISO/IEC 27018 and other specifications for hosting of health data.

There will be a two-step procedure: first documentary audit, followed by an onsite audit. Certification is granted for 3 years and there will be a yearly audit by the certification body.

- **Contracts**

The Decree, in the new Article R1111-11, lists what the hosting of data agreement must contain, including with respect to security of and access to the data.

Transition period:

- Authorisations obtained or applied for with the French Ministry before 1 April 2018 will continue to be valid until the end of their 3 year term;

- Companies which authorisation end less than one year after 1 April 2018 are granted an additional 6 month period for obtaining the new certification; and

- Any application made after 1 April 2018 will be for a certification.

There are still grey areas regarding requirements for outsourcing services, especially for services providers that did not need an authorisation, but now may need to be certified. Further guidance is expected soon.

Sanctions

Breach of Article L.1111-8 of the Public Health Code is sanctioned by up to 3 years imprisonment and a fine of € 45,000 in case of individuals and € 225,000 in case of

legal entities.

Processing of personal data in such circumstances may also be sanctioned by the French data protection authority (the “CNIL”), that can impose a fine of up to € 3 million (and after 25 May 2018, up to €20 million or 4 % of the worldwide turnover), as well as an injunction to cease processing. Sanctions are made public. The CNIL has already issued a sanction in relation a health data hosting service provider.

Breaches to data protection regulations or to professional secrecy can also give rise to criminal fines.

It is essential that Article L.1111-8 be taken into account when dealing with certain types of health data of French residents.