# Data Protection Investigation in the Hospitals Sector

A report by the Special Investigations Unit of the Data Protection Commissioner's Office following an investigation conducted under section 10(1A) of the Data Protection Acts, 1988 & 2003.

May 2018

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

# Contents

Overview and Scope 3

Overall Investigation Report 7

Matters of Concern 9

- Controls in Medical Records Libraries 10
- Security 15
- Storage of Patient Observation Charts in Hospital Ward Settings 23
- Storage of Patient Charts in Trolley Bins in Ward Settings 26
- Storage of Confidential Waste Paper Within the Hospital Setting 29
- Disposal of Handover Lists and Patient Lists 31
- Use of Fax Machines 33
- Lack of Speech Privacy 35
- Absence of Audit Trails 38
- Raising Awareness of Data Protection in Hospitals 41
- Consent for Research 45
- The Processing of Private Health Insurance Information in Hospitals 47
- Maternity Service Users 51
- Data Retention 53

Executive Summary 55

Conclusion 68

# A Data Protection Investigation in the Hospitals Sector: Overview and Scope

In January 2017 the Special Investigations Unit set out in a scoping document the purpose, focus, aim and scope of this investigation in the following terms:

## Purpose of Investigation

The purpose of this special investigation is to examine the journey of sensitive personal data held on patient files and patient charts within the Hospitals Sector and to determine if patient care is delivered in a manner that gives due respect to the legitimate data protection rights and expectations of patients.

It has been decided to explore this issue from a patient's perspective. It is our intention to inspect a range of hospitals across the State to assist the Data Protection Commissioner to gain a meaningful insight into patients' interface within the Hospitals Sector.

With the benefit of increased staffing resources for the Data Protection Commissioner's office, the Special Investigations Unit was established in 2015 primarily to carry out investigations on its own initiative, as distinct from complaints-based investigations. The Special Investigations Unit decided to conduct this special investigation of the hospitals sector arising from a number of factors such as the substantial volume of sensitive personal data which is processed on an ongoing basis in that sector; our awareness of some significant data security breaches in the sector in the previous decade; and the findings of data protection audits conducted in a number of hospitals by our Audit Unit in recent years.

Health information falls into the category of "sensitive personal data" within the meaning of the Data Protection Acts ['The Acts']. The Acts set down additional conditions for the processing of sensitive personal data and data controllers, therefore, are obliged to treat sensitive personal data with a high level of duty of care.

## Focus of Investigation

The investigation will examine the processing of patient sensitive personal data in departments and areas of hospitals in Ireland to which patients and the public have access.

It will involve physical inspections at hospitals in different parts of the State spanning HSE facilities, private hospitals and voluntary hospitals to give as broad an insight as possible into the processing of sensitive personal data in public areas of hospitals.

The investigation will concentrate as far as possible on the circulation and journey of patient charts and medical files in order to identify if there are any shortcomings in terms of meeting the requirements of The Acts to keep personal data safe and secure and to have appropriate measures in place to prevent unauthorised access to or disclosure of personal data.

## Aim of Investigation

Based on the findings of the investigation and where issues of concern are identified with regard to data protection compliance, the aim is to make recommendations for improvements with regard to the processing of patient sensitive personal data not only in the hospitals which are selected to participate in the investigation but across the hospitals sector in general.

It is anticipated, therefore, that recommendations will fall into two broad categories. Firstly, there may be recommendations that are specific to individual hospital facilities. These recommendations will be conveyed to the hospital concerned as soon as practicable after the inspection.

Secondly, there may be recommendations that will apply to the whole hospitals sector or to groups of hospitals. These recommendations will be formulated at the end of the inspections process taking into account the cumulative findings of all of the inspections undertaken. These recommendations will form part of an overall investigation report that will be compiled following completion of the inspections process. That investigation report will be issued to all major hospitals across the State.

## Scope of Investigation

- The investigation will commence in January 2017.
- The investigation will cover HSE facilities, private hospitals and voluntary hospitals across the State.
- Inspections will be carried out by Authorised Officers of the Data Protection Commissioner. The first phase will involve the inspection of a minimum of fifteen hospital facilities spanning the full geographic area of the State. On completion of the first phase of inspections, consideration will be given to a second phase involving the inspection of further hospital facilities. Inspections will commence in January 2017 with an expected completion time-span of twelve months.
- The investigation will concentrate on major hospitals that have a range of patient departments.
- During the course of the inspection, the Inspectors will first seek to meet with relevant hospital management staff to get an overview of the facility and its policies and procedures with regard to data protection compliance in respect of patient sensitive data. Secondly, the Inspectors will seek to obtain copies of blank patient charts, data protection policy documents and patient confidentiality obligations imposed on staff. Thirdly, the Inspectors will visually inspect areas and Departments in the hospital facility to which patients and the general public have access to identify and follow the journey of patient charts and patient files in each area in order to establish if there are shortcomings in terms of meeting the requirements of The Acts. Finally, the Inspectors will visually inspect the hospital's Medical Records Office to examine the processing of patient charts and files in that Office, including electronic filing systems, and to get an overview of the safety, security and file control systems that are in place at the hospital facility.
- The inspections will concentrate primarily on the data protection obligations on data controllers to keep personal data safe and secure and to have appropriate measures in place to prevent unauthorised access to or disclosure of personal data. In carrying out physical inspections, the inspectors will focus their attention particularly on any potential risks they can identify with regard to the disclosure, in any manner, of patient sensitive data to third

parties and on any potential risks they can identify with regard to vulnerabilities concerning the safety and security of such data.

## List of Hospitals at which Inspections were Carried Out.

- Royal Victoria Eye and Ear Hospital, Dublin
- Mater Misericordiae Hospital, Dublin
- Beaumont Hospital, Dublin
- Our Lady's Children's Hospital, Crumlin, Dublin
- Adelaide & Meath Hospital incorporating the National Children's Hospital (Tallaght)
- Blackrock Clinic, Blackrock, Co. Dublin
- National Maternity Hospital, Holles Street, Dublin
- St. Vincent's University Hospital, Elm Park, Dublin
- Midlands Regional Hospital, Mullingar, Co. Westmeath
- Aut Even Hospital, Kilkenny
- St. Luke's Hospital, Kilkenny
- Our Lady's Hospital, Navan, Co. Meath
- Wexford General Hospital, Wexford
- Bon Secours Hospital, Cork
- Cork University Hospital, Cork
- University Hospital Kerry, Tralee, Co. Kerry
- University Hospital Limerick
- Sligo University Hospital, Sligo
- University Hospital Galway
- Letterkenny University Hospital, Letterkenny, Co. Donegal

The Data Protection Commissioner wishes to acknowledge the high level of cooperation her Authorised Officers received from the management and staff of all of the hospitals listed above when carrying out their inspection work.

Subsequent to the inspection, the Special Investigations Unit issued an inspection report to each of the above hospitals. Each report contained several recommendations and each hospital has been asked to submit an action plan to the Data Protection Commissioner in relation to the implementation of the recommendations.

# Overall Investigation Report

This overall investigation report draws from the contents of the individual inspection reports that were issued to twenty hospitals in the State following the inspections conducted by the Special Investigations Unit in 2017.

This report sets out of the key matters of concern that the inspection teams identified across the twenty hospitals inspected and it outlines the recommendations made by the Special Investigations Unit to the hospitals concerned to deal with those matters of concern.

In this report, we are intentionally not identifying by hospital the specific matters of concern that arose in each of the twenty hospitals inspected. Many of the matters of concern arose in several of the hospitals inspected while a small number of the matters of concern were particular to a handful of hospitals inspected.

Over the course of this investigation, the Special Investigations Unit carried out inspections of a broad range of facilities spanning HSE hospitals, private hospitals and voluntary hospitals. On a geographic basis, the twenty hospitals inspected represent a broad sample from across the State with eight hospitals inspected in the Dublin area, five hospitals inspected in the greater Leinster region, two hospitals inspected in Connacht, four hospitals inspected in Munster and one hospital inspected in Ulster.

Given the breadth of this special investigation both in terms of the range and the geographical spread of the facilities inspected, it follows that the matters of concern identified during those inspections are ones that likely currently arise in other hospital facilities throughout the State.

The primary purpose of this overall investigation report is two-fold. Firstly, its purpose is to bring to the attention of every hospital in the State the matters of concern that our inspectors found in the sample of twenty hospitals inspected. Secondly, its purpose is to prompt every hospital in the State to examine whether any or all of the issues highlighted in the matters of concern in this report are occurring or could occur in its facility and, if so, to implement the recommendations we are making to remedy the situation. In examining whether any or all of the matters of concern are occurring or could occur in its facility, each hospital is advised to consider every part of the entire hospital campus as part of its examination in order to establish the relevancy, if any, of each of the risks and recommendations in each area. The implementation of the recommendations will not be achieved by simply issuing reminders to staff or by creating standard operating procedures. Rather, it will be necessary for each hospital to support the implementation of the recommendations by putting in place the necessary infrastructure and resources that may be required as essential enablers.

For our part, we will issue this report to every hospital in the State and we will request them to consider which matters of concern arise or could arise in their facility. We will also issue them with a template quality improvement action plan as a tool to assist them in identifying the data protection risks relevant to their facilities and to aid them in deciding the remedial actions they intend to take to mitigate those risks.

# Matters of Concern

# Controls in Medical Records Libraries

## Context

One of the key tasks in this investigation was to inspect the various repositories in which hard-copy patient charts are stored. Across the hospital system, different terms are used to describe these repositories but for the purpose of this report they will be referred to as "Medical Records Libraries."

Medical Records Libraries provide a critical and essential function with regard to the safe-keeping of physical patient charts. Usually these Libraries are located in a part of the hospital facility to which patients or other members of the public do not have access. Medical Records Libraries are normally staffed full-time during office hours and depending on the size of the hospital, staff numbers can range from four or five to over twenty. In some large hospitals, there are staff on duty in Medical Records Libraries at all times including at weekends and overnight. The volume of charts in storage depends on the available space. However, even hospitals that have limited storage space usually have several thousand patient charts in their Medical Records Library. Most hospitals use off-site storage for charts that have been out of use for a particular period of time.

Overall, the inspectors found that there is scope for much greater security controls with regard to Medical Records Libraries in light of the fact that physical patient charts contain the most detailed clinical records in relation to the patient's care, condition and treatment at the hospital. It is critical that hospital management do not underestimate the potential risks that can arise with regard to laxity in relation to security controls.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

In some instances, controls were lax with regard to restricting access to the Medical Records Library by hospital staff who are employed in other parts of the hospital. In one hospital the internal postal facilities room was situated in the same area as the Medical Records Library. In effect in that instance, any hospital staff member who had access rights to enter the postal facilities room had unrestricted access to the Medical Records Library. In another instance, every staff member in one hospital who carries a door swipe card has access to every area of that hospital, including access to the Medical Records Library. The inspectors noted two hospital situations where up to three thousand staff had access to the Medical Records area of the hospital in one instance and up to sixteen hundred staff had access to the Medical Records area in another instance. Any deficit in restricting access to the Medical Records Library of a hospital by staff who have no ongoing business need to enter that area poses the very serious potential risk that staff members could enter the Library to snoop through medical charts of family members, friends or others out of sheer nosiness or for other more sinister purposes. Because the charts are physical rather than electronic in form, the risk is compounded by the fact that such snooping could go undetected unless it was witnessed by another party.

### *Recommendations*

- Robust controls should be put in place to limit staff access to the Medical Records Library to those hospital staff who have a current business need for such access. It is critical that every hospital in the State review its current security controls to identify any potential weaknesses and to take remedial action to tighten access controls to the maximum extent possible.

- To keep the number of staff who have access to the Medical Records Library to a minimum, other units or departments of the hospital should not be physically located in the same area unless robust access control measures are in place to restrict staff access to the Medical Records Library.

### Risk No. 2

Only a small number of the inspected hospitals have a means to record staff access to their Medical Records Libraries. The remainder had no means of monitoring unauthorised staff access. Unmonitored access to the Library area of a hospital containing the most sensitive personal data of thousands of patients lends itself to a high risk of unauthorised access by staff who have no business reason to enter the area. That staff are aware that access to the Library is unmonitored could act as a temptation for them to access that area for nefarious purposes.

*Recommendations*

- A procedure should be put in place to routinely generate access reports in respect of staff access to the Medical Records Library. These access reports must be monitored on a regular basis to detect if any suspicious patterns of access are occurring.

- It is critical that hospital staff are made aware that the Medical Records Library is generally out of bounds for all staff, with the exception of those who have authorised access for business purposes. For deterrent purposes, it is essential that all staff are made aware that access to the Medical Records Library is regularly monitored.

- To deter staff from accessing patient charts without a business reason for doing so, hospitals should devise policies that treat such unauthorised access as a disciplinary matter.

### Risk No. 3

Practices varied in the hospitals inspected with regard to ‘after-hours’ staff access and accountability for charts removed from the Medical Records Library during ‘after-hours’ periods. In many cases, no logs were created to record details of who entered the Library or details of which chart they removed. There was little evidence of any restriction on a staff member who has access to the Library ‘after-hours’ from bringing an ‘unauthorised’ staff member to the Library with them.

*Recommendations*

- For access to the Medical Records Library ‘after hours,’ a log book or similar should be implemented in which staff members who access the Library must sign in and sign out. In this log book they should also record by chart number, date and time, details of the charts they have removed from the Library.

- Staff who are authorised to access the Medical Records Library should be prohibited from bringing an unauthorised staff member into the Medical Records Library with them.

## Risk No. 4

The Medical Records Library in most hospitals inspected had no alert system in place to draw attention to charts which had been previously removed from, but not been returned to, the Library by a certain period of time.

### *Recommendations*

- A procedure should be put in place on the electronic patient management system to routinely generate reports in respect of medical charts that have not been returned to the Medical Records Library by a certain period of time.

- It is critical that these reports be monitored in an effort to establish the current location of the medical charts concerned and to allow for the updating of the electronic patient administration system to reflect the current location of the patient chart.

## Risk No. 5

Open top trolleys (on four wheels) are commonly used to transport patient charts from the Medical Records Library to the various hospital departments where they are required. Most hospitals reported that the general practice in this situation is that the staff member in control of the trolley turns the charts face down to ensure that the personal details on the front cover cannot be read. Despite this practice, patient charts that are transported in an open-top trolley from the Library to another location of the hospital via corridors, lifts and wards are particularly vulnerable to exposure. In a busy public area of a hospital, there is a high risk that the staff member in control of the trolley could become distracted or otherwise engaged, thus bringing the security of the patient charts into question.

### *Recommendations*

- Trolleys used to transport medical charts throughout the hospital facility should be covered over securely to protect the patient information held on the medical charts from being seen or accessed by third parties.

- Medical charts should not be stored outside the secure bin compartment of trolleys while trolleys are in transit.

- On a general level, robust procedures should be put in place with regard to the movement of medical charts throughout the hospital to ensure that staff protect the personal data on medical charts from being seen by other parties.

### Risk No. 6

In some hospitals inspected, there was no electronic tracking of chart movement. Instead, the monitoring of chart movement was based solely on a manual system of updating a tracer card in the Medical Records Library. In one instance, updates to the tracer card were triggered by telephone calls to the Medical Records Library from staff involved in the movement of the chart in the various hospital departments. Such a manually operated system presents a significant risk that chart tracking may not be up-to-date with the added risk that if a chart is required urgently, its current location may not be readily identifiable.

### *Recommendation*

- Manual systems for the tracking of patient charts should be replaced by electronic tracking systems, incorporating features such as bar-coding, that have the capacity to accurately identify the location of all patient charts at all times.

# Security

## Context

In general, rigid controls are in place in hospitals to restrict public access to certain parts of hospital facilities. However, as outlined below, some concerns were noted in that regard during the course of the hospital inspections.

Computer workstations are an essential and prominent feature of the hospital environment and it is critical that appropriate security features and procedures are implemented to safeguard the substantial volume of personal and sensitive personal data that are processed at such workstations on an ongoing basis.

In some hospitals inspected, there was scope for improved security measures in relation to the handling and storage of patient charts and other forms of patient information. For example, in one hospital on the corridor of a public ward, patient charts of current patients were stored in an unlocked glass cabinet. On further inspection, a patient medical chart of a discharged patient was found disregarded on top of the glass cabinet. On the same ward, the inspectors observed two cardboard boxes containing patient charts of discharged patients. These charts were awaiting transmission onwards to the Medical Records Library and the inspectors were informed that it was standard practice that charts of discharged patients would be stored in this way on the ward for up to one week. In these examples, the patient charts could easily be accessed by patients, visitors or other members of the public.

When the General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 there will be a legal requirement on all data controllers to notify the Data Protection Commissioner of personal data security breaches.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

Some inspections noted areas of weakness in relation to access controls on some doors leading to restricted areas. In some instances also, door access logs were insufficiently monitored. In another instance every staff member in one hospital who carries a door swipe card has access to every area of that hospital (For example, it is questionable why Emergency Department staff would have access to the Outpatients Department or a Day Case Ward and vice versa). Weaknesses in relation to the security of doors and wide-ranging levels of swipe card access has the potential to jeopardise the safe-keeping of patient charts that may be stored in the affected areas and thereby put personal data and sensitive personal data at risk of unauthorised access.

*Recommendations*

- Door access to all areas of the hospital to which patients or members of the public do not have general access should be properly secured at all times to prohibit access by unauthorised persons.

- Swipe card access, where this is in place, must be properly planned and monitored across the whole hospital campus to ensure that staff are restricted, in line with their respective job roles, from entering areas that they have no business need to access.

- Where swipe card access controls are in use, these should be reviewed regularly (every six months at a minimum) to ensure that only those staff who have a current need to access the areas of the hospital concerned are enabled to do so.

- Security procedures should be implemented to generate access logs in relation to doors leading to restricted areas. These access logs should be audited regularly to detect patterns of unusual or unauthorised accesses.

- Where key pad access controls are in use, the key codes should be changed periodically.

- Security access mechanisms on doors should be tested regularly to ensure that they are functioning properly.

- Consultation Room doors should always be closed while patients are attending a medical consultation in order to protect their data protection rights.

- Keys of locked offices should be stored in a secure location and staff should be prohibited from taking such keys home at the end of their shift.

### Risk No. 2

Concerns arose also in relation to some computer workstations. In a number of instances, personal data on computer screens was viewable by passers-by due in the main to the physical positioning of the computer screen.

*Recommendation*

- Personal data on computer screens should be hidden from the view of passers-by at all times.

### Risk No. 3

In other instances, a lack of appropriate technical safeguards resulted in unattended computer screens remaining open for lengthy periods of inactivity. In these circumstances, other staff and members of the public who may be in the vicinity at the time (e.g. a person accompanying a patient in the Emergency Department) may be able to view the personal data on the open screens. Furthermore, staff failing to log off after use could result in the next user inputting information using the previous user's account.

### *Recommendations*

- Appropriate security measures should be implemented to ensure that computer screens are set to automatically lock and log users off after a certain short period of inactivity. In that regard, consideration should be given to the business needs of the different work areas within the hospital in determining the appropriate maximum time-out periods. For example, across the hospital facility time out periods could vary between one minute in one area and ten minutes in another area, depending on the business needs of each area.

- A screen saver should appear on locked screens to ensure that no personal data of patients remains visible.

- Staff should be prohibited from accessing or editing, via other users' accounts, the records of personal data on hospital computer systems.

## Risk No. 4

Several issues of concern were identified in relation to the handling and storage of patient data. These included the storage of patient charts in unsecure filing cabinets; the storage of emergency department cards ('ED' cards) in Emergency Departments for indefinite periods; the storage of keys of filing cabinets used for the filing of patient charts or files in insecure locations; the use of see-through plastic holders mounted on walls to store patient information; the leaving of patient charts on shelves or tables outside of consultation rooms in Outpatient Departments; the leaving of patient charts on counter-tops in various hospital reception areas; and the leaving of confidential correspondence in unattended areas.

### *Recommendations*

- All filing cabinets used to store patient charts or other personal data of patients should be locked securely to prohibit unauthorised access.

- Keys of locked filing cabinets should be stored in a secure location and staff should be prohibited from taking such keys home at the end of their shift.

- 'ED' cards which are created routinely in hospital Emergency Departments to record details of the patient's attendance should be kept in the Emergency Department for a limited period before being sent to the Medical Records Library or other secure environment for filing.

- The practice, which is common in many Outpatients Departments, of storing patient charts in a casual or an unprotected manner on shelves or tables outside of consultation rooms while the patient awaits calling by the medical team should be discontinued and the patient charts should instead be kept in a more secure environment where they are not at risk of being accessed by third parties. [As an example of good practice, in one hospital the inspectors noted that patient charts were stored outside the consultation rooms in a secure trolley bin, the lid of the trolley bin was closed over, charts were not stored outside the trolley compartment unit, and the trolley bins were located at a safe distance from waiting patients. In addition, a staff member was on duty in this area whose function it was to facilitate the orderly flow of patients to the relevant consultation room and to have oversight of the safe-keeping of the patient charts].

- Confidential information regarding patients must be guarded securely at all times and security measures must be implemented to ensure that such correspondence is not left lying around in environments in which they can be easily accessed by passers by.

- In a number of hospital facilities, patient medical charts were stored in unlocked cabinets or open shelving in areas such as the Admissions Office, the Outpatients Department or corridors areas or sub-offices within the Medical Records Library. Cease practice of storing patient medical charts in unsecured areas and ensure that all medical charts currently held in an unsecure environment are moved to a secure area.

## Risk No. 5

A practice of requiring patients who check-in to hospital via an Admissions Office to carry their medical chart to the ward to which they are assigned was particularly common in many of the hospitals inspected. Given the sensitive nature of the information which may be contained in a patient's medical chart coupled with the patient's natural anxiety about checking in to a hospital for a procedure or treatment, this practice presents a real risk to the safety of the chart while it is in the custody of the patient. This risk continues to exist where the hospital supplies sealed bags into which the patient chart is placed before being handed to the patient to carry to the relevant ward.

### *Recommendation*

- Procedures should be introduced in hospitals to ensure that patients are never required to carry their medical chart from one part of the hospital to another. This function should be carried out by hospital staff in all circumstances.

## Risk No. 6

When the GDPR comes into effect on 25 May, 2018 there will be a legal obligation under Article 33 for data controllers to notify the Data Protection Commissioner of personal data breaches. Mandatory breach notification entails the reporting of all breaches to the Data Protection Commissioner, typically within seventy two hours, unless the data controller can demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals. Furthermore, under Article 34 of the GDPR, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller is obliged to inform the data subject of the breach without undue delay.

These onerous responsibilities require that data controllers have robust protocols in place to ensure that they comply fully with the GDPR breach notification requirements. On the evidence of some of the inspections, there is a potential risk that some hospitals may not have such breach protocols in place and on time. In that regard, considerable work needs to be done to develop and implement the breach notification protocols in each hospital and to train and inform staff in relation to the requirements.

### *Recommendations*

- A protocol to handle personal data breaches should be in place in every hospital by 25 May, 2018.

- Hospital staff should be trained fully on the implementation of the data breach protocol. They should be educated on how to recognise data security breaches and they should be given simple, clear instructions on what to do in the event of a data security breach.

## Risk No. 7

In one hospital inspected, concerns arose about items of incoming and outgoing postal correspondence that, as standard practice, were left in unsecured wire trays in an unprotected environment while awaiting collection by hospital porters. The inspectors were concerned that there was a high risk that the personal and sensitive personal data of patients that was contained in the postal correspondence could easily be inappropriately accessed by patients or visitors. In another instance, postal correspondence was left in an open unsecured tray on a counter top in a public ward where passers-by could easily access it.

### *Recommendation*

- Postal correspondence, such as incoming and outgoing letters, that is awaiting collection or further distribution within the hospital setting, should be held in a secure environment out of reach of patients or visiting members of the public.

## Risk No. 8

Almost all hospitals inspected use third party service providers for the storage of physical medical charts that have reached a certain age. In one hospital inspected, confusion arose in relation to whether or not a contract was in place with the off-site storage service provider.

*Recommendation*

- All data processing arrangements with third party service providers should be reviewed to ensure that the contracts meet the requirements of Section 2C(3) of the Data Protection Acts 1988 & 2003 and that they will meet the requirements of the GDPR from 25 May, 2018.

# Storage of Patient Observation Charts in Hospital Ward Settings

## Context

Observation charts are widely used in hospitals throughout the world. These are essential documents that allow for the recording of patient physiological observations during their hospital stay.

Varying levels of physiological details may be recorded on observation charts depending on the type of chart used. Most observation charts are used to monitor, at a minimum, the patient’s vital signs such as body temperature, heart rate or pulse, respiratory rate and blood pressure. Usually the patient’s full name and date of birth are recorded on the observation chart.

The physiological details recorded on an observation chart in respect of an identifiable patient renders the content of the chart to fall into the category of ‘sensitive personal data’ within the meaning of the Acts. For the purposes of the GDPR, such physiological details fall into the definition of ‘data concerning health.’

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

In some of the hospital facilities inspected, as standard practice, patient observation charts in respect of admitted patients are clipped to the end of each patient’s bed. Where the patient is admitted to an isolation ward, it is standard practice in some hospital facilities to hang the patient’s observation chart on a wall rail immediately outside of the patient’s isolation ward, usually in a corridor area. In both of these situations, as the observation charts are unprotected and unsecured there is a high risk that the observation charts of patients could be viewed or accessed inappropriately by third parties such as other patients, visitors or other members of the public.

As data controllers, hospitals are obliged to take appropriate security measures against unauthorised access to or disclosure of personal data. The practices outlined above are inherited ones that pre-date data protection law. Unfortunately, these practices lend themselves to situations whereby the personal data of patients is exposed to snooping third parties, such as visitors in particular. Patients have a right to have their personal data that is recorded on observation charts fully protected and the responsibility for protecting that personal data rests with the hospital concerned.

It will be a matter for each hospital that engages in the practices outlined above, or similar, to find and implement a solution which fully protects the personal data of patients while, at the same time, meets the hospital's needs in terms of accessibility of the observation charts for nurses and clinicians. However, it will not be acceptable to attempt to implement the following recommendations by a minimalist form of action such as placing a blank sheet of paper on the top of the patient observation charts, or by placing the patient observation charts in unsecured folders or other forms of unsecured devices. Key to the successful implementation of these recommendations will be securing all patient observation charts in a manner that protects them from being accessed by other patients, visitors, passers-by or other third parties.
***[It is worth noting that in a small number of the hospitals inspected, patient observation charts were stored securely in all cases in the Nurses' Station of the respective ward].***

## Recommendations

*[NOTE: The implementation by hospitals of these recommendations should take into account issues that relate to patient safety in ward settings to ensure that an appropriate balance is achieved between mitigating the data protection risks outlined above and mitigating risks to patient safety].*

- Where patient observation charts are currently clipped to or left hanging on the ends of patient beds, they should in future be stored securely in a protected environment, in the immediate vicinity of the patient's bed if necessary, where they are accessible only to hospital staff who have a professional need to access them.

- Where patient observation charts are stored on wall rails or similar outside of isolation wards or isolation rooms, they should in future be stored securely in a protected environment, in the immediate vicinity of the patient's ward or room if necessary, where they are accessible only to hospital staff who have a professional need to access them.

# Storage of Patient Charts in Trolley Bins in Ward Settings

## Context

A Healthcare Record, commonly known as a Patient Chart, is normally created for every admitted patient in hospitals across the State. The patient to whom the chart relates is usually identified by means of a label affixed to the front cover. The label shows details of the patient's name, address, date of birth and healthcare record number. Typically, a chart is a folder consisting of patient information that is placed in a relevant section within the folder. For example, the sections of the chart may be ordered along the following lines: Adminstration Section, Correspondence Section, Clinical Notes Section, Nursing Notes, Procedures, Consent, Clinical Measurement, Laboratory Results, Radiology & Diagnostic Imaging Results, Prescribed Medicines and Health & Social Care Professionals Section.

The details recorded on a patient chart in respect of an identifiable patient clearly renders the content of the chart to fall into the category of 'sensitive personal data' within the meaning of the Acts. For the purposes of the GDPR, such details fall into the definition of 'data concerning health.'

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

In the ward setting of some of the hospitals inspected, patient charts of the current admitted patients are stored in what are known as chart trolley bins. Trolley bins come in various shapes and sizes. Most trolley bins are mobile (with four wheels) and they have lockable lids. Some have open shelving space at the bottom underneath the closed storage unit. In a ward setting, trolley bins are usually kept immediately outside or within the Nurses' Station. During the daily 'doctor's rounds' when clinical teams tour the wards, the trolley bins are used to bring the patients' charts on the rounds.

While the patient charts that are stored in trolley bins can be securely protected from unauthorised access by closing and locking the trolley bin lids, the inspectors found little evidence in some hospitals that the trolley bin lids were ever used for this purpose. More commonly, the trolley bin lids were used by medical professionals as an aid to leave the patient's chart on when writing up case notes on the chart. Of particular concern were situations where the unlocked trolley bins were parked outside of the Nurses' Station where the patient charts within them could potentially be accessed by passers-by such as patients, visitors or other members of the public.

### *Recommendations*

- All trolley bins that are used in ward settings to store patient charts of current patients should be kept within a secure area out of reach of passers-by, such as behind the desk in the Nurses' Station or in a locked office space.

- During public visiting times, the lids of all trolley bins containing patient charts should be closed over and locked.

### Risk No. 2

In some hospitals, the inspectors noted instances where patient charts and/or patient information or nursing notes were stored in an unprotected environment either in the open shelving space at the bottom of the trolley bins or in hanging devices at the side of trolley bins.

### Recommendation

- Patient charts, patient information or nursing notes should never be stored in open shelving on trolley bins.

# Storage of Confidential Waste Paper Within the Hospital Setting

## Context

As in many working environments, the storage and disposal of confidential waste paper features prominently in hospital settings. Confidential waste is created in almost every area of a hospital facility on a daily basis. Given the nature of the work carried out in a hospital environment, it follows that much of the confidential waste relates to patients in terms of personal information relating to their medical condition, treatment, health insurance, medical appointments, etc.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

Several hospitals that were inspected use paper bins, bags or trays that are not secure in offices, sections and wards throughout the facility. Typically, in these situations, waste paper that is placed in these bins, bags or trays can be removed by others. For example, in one hospital the inspectors observed a staff member removing a binned confidential document which contained patient information that had earlier been placed in an unsecure bin by a different staff member.

In a modern working environment, where a data controller is processing significant volumes of personal data or sensitive personal data and is generating confidential waste from such data processing activities, it is incumbent on that data controller to deploy secure confidential waste bins to appropriately protect the personal data concerned from unauthorised access or disclosure.

### *Recommendation*

- Replace all unsecure bins, bags and trays that are used to store confidential waste paper with secure lockable confidential waste bins that have a bin top or slot through which confidential waste can be placed but not retrieved. This recommendation applies to all areas of the hospital facility including office areas to which access is restricted to staff.

# Disposal of Handover Lists and Patient Lists

## Context

In ward settings of several, but not all, hospitals inspected nursing staff carry physical paper lists in the pockets of their uniforms for the duration of their shift. Some hospitals use the term ‘handover lists’ to describe these lists as they are compiled when one nursing shift is handing over to the next nursing shift. During that handover briefing session the incoming shift nursing staff make a written note of various aspects of nursing care for each patient on their ward. Other hospitals use the term ‘patient lists’ as, in those cases, the lists contain minimum information such as the name and bed number of each patient.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

All hospitals whose nursing staff use either handover lists or patient lists in the ward setting reported to the inspectors that it is standard procedure that, at the end of each shift, nurses place the lists in a shredder or in a confidential waste bin. However, the inspectors found no evidence that any of the hospitals concerned monitor compliance with the standard procedure. Accordingly, in the absence of an end-of-shift procedure to account for the secure disposal of such lists, there is a significant risk that nursing staff may inadvertently take the lists out of the hospital setting at the end of their shift and dispose of them at a later point elsewhere. As lists of this nature contain personal information on patients that may be particularly sensitive, it is essential that they are securely disposed of in the hospital environment. For that reason, hospitals must have a means of accounting for the collection of each list at the end of each shift and their safe disposal in a shredder or in a secure lockable confidential waste bin.

***[It is worth noting that in a small number of the hospitals inspected handover lists or patient lists are not created or used on every ward and those wards function effectively without them]***.

## Recommendations

- Implement a robust procedure in ward settings to ensure that all used handover lists and patient lists are accounted for at the end of each shift and that they are all disposed of safely in a shredder or in a secure lockable confidential waste bin. This can be achieved, for example, by providing a sign-off sheet at the shredder/confidential bin where staff sign that they have completed the safe disposal of the lists.

- Otherwise, discontinue the practice where nursing staff carry physical paper handover lists or patient lists in the pockets of their uniforms.

# Use of Fax Machines

## Context

Fax machine usage for the transmission of written messages continues at a relatively high rate in many of the hospitals inspected. The inspectors noted fax machine usage in several hospital departments such as Emergency, Outpatients, Admissions and in Nurses' Stations of many inpatient wards. Fax machines are regarded as an essential communications tool in many hospitals to transmit patient information to and receive patient information from general practitioners, nursing homes and other hospital facilities. The level of fax machine usage remains high despite the availability of encrypted email as a more secure method of electronic communication.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

One of the biggest risks associated with the use of fax machines is human error when dialling the number to send an outgoing fax message. Several data security breaches have been reported to the Data Protection Commissioner as a result of such errors, including incidents involving the transmission of patient information between hospitals and medical practitioners. Particular risks arise around dialling the digits in the correct order as well as omitting to dial or incorrectly dialling the area code of the receiving fax number.

*Recommendation*

- Where possible, regularly dialled fax numbers should be pre-programmed into the fax machine to minimise the risk of mis-dialling errors. Where this is not possible, a directory of regularly dialled fax numbers typed in a clear and easy-to-read format should be placed in a prominent position beside each fax machine.

### Risk No. 2

The inspectors noted of lack of guidance for fax machine users in many hospitals to inform them of best practice with regard to the sending or receiving of fax messages containing sensitive personal data.

*Recommendation*

- All fax machines should have a guidance note on display nearby to provide users with advice on the circumstances in which it is appropriate to use fax machines to transmit personal or sensitive personal data and to warn users of the risks of transmitting the message to the wrong fax number. The guidance note should also provide practical directions on how to use a fax machine. It should outline the procedures to be followed in the event that an outgoing fax message is mis-directed.

# Lack of Speech Privacy

## Context

Speech privacy is usually defined as the inability to understand conversations, although some words may still be audible. Speech privacy is achieved when speech, or conversations between two or more parties, cannot be understood by other individuals who may be in close proximity.

One of the most common matters of concern noted in the hospital inspections carried out in 2017 was the lack of speech privacy in various areas of hospital facilities. This issue arose in many different areas of hospitals where patients interacted with hospital staff such as at reception desks in Emergency Departments, reception desks in Outpatients Departments, treatment cubicles in Emergency Departments, at hospital beds on wards. In many cases, the lack of speech privacy could be attributed to either the general layout of the area concerned or to the limited space available in the area concerned.

In short, patients should be afforded the privacy to discuss their medical condition, their medical treatment, their financial arrangements with the hospital, their private health insurance status or medical card status, and all other personal matters with hospital staff without the risk of being overheard by others.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

In those areas of hospitals where the inspectors noted a lack of speech privacy, there existed a real potential for third parties such as other patients and hospital visitors, to over-hear private conversations between patients and hospital staff. Take, for example, the reception desk scenario. Arriving patients are usually requested by hospital receptionists to verbally provide several elements of their personal data such as name, address, date of birth, contact details, next of kin details, medical card details, etc. The receptionist then inputs the details supplied by the patient to the hospital computer system. This engagement at a hospital reception desk obviously constitutes a form of data processing. The hospital, which is the data controller, is obliged to take appropriate secure measures against disclosure of personal data. In the scenario of the reception desk described above, the hospital must ensure that a patient's engagement with a receptionist and the collection of personal data that takes place during that engagement is conducted in an environment that affords the patient adequate speech privacy and protects against the disclosure of their personal data to other parties in close proximity.

### *Recommendations*

- In reception areas, patients should be afforded sufficient space and privacy to allow them to provide details of their personal information to hospital staff without the risk of being over-heard by by-standers or passers-by.

- A range of solutions should be considered in reception areas to render speech unintelligible to the casual listener such as a review of the general layout of the area concerned, the posting of privacy notices on adjacent walls, the painting of line markings on floors, the introduction of appropriate sound/acoustic technologies and the use of a ticketing system which would reduce the possibility of others standing immediately behind the patient who is checking in.

- When check-in areas are on public corridors, a range of measures should be introduced such as placing dividers between hatches at the check-in desk, line markings on floors, etc. If necessary, the positioning of the check-in desk should be altered to make it a more privacy-friendly environment or consideration should be given to relocating it to a different part of the hospital where the speech privacy risks will not arise.

## Risk No. 2

Another striking example of the lack of speech privacy noted by the inspectors occurred in the treatment cubicles of some Emergency Departments. The cubicle setting in several Emergency Departments inspected comprised a curtained area of limited size with partitions on either side. Private conversations taking place in these cubicles between medical staff and patients could easily be overheard in the adjoining cubicles at either side. Discussions of a most sensitive nature take place between medical staff and patients in treatment cubicles of Emergency Departments around matters such as symptoms, previous medical history, treatment plans, etc.

By way of another example, in one hospital the inspectors overheard a conversation about a patient's medical condition and treatment plan as it occurred between a doctor and a patient on a corridor area of an inpatient ward. It is incumbent on hospitals, therefore, to ensure that engagements of this nature between patients and medical staff are conducted in a privacy-friendly environment that adequately protects the personal and sensitive personal data of patients.

### *Recommendations*

- In treatment areas, hospital wards and other areas of hospitals, patients should not be expected to discuss with medical or other hospital staff their medical condition, medical care or treatment or any other aspects of their personal information in environments where their speech privacy cannot be respected.

- A range of solutions should be considered to render speech unintelligible to the casual listener such as a review of the general layout of the area concerned, the posting of privacy notices on adjacent walls, the painting of line markings on floors, the introduction of appropriate sound/acoustic technologies and the use of enhanced privacy curtains, among other things. These solutions should be implemented as a package in order to have maximum beneficial effect. Selecting and implementing one solution in isolation is unlikely to achieve maximum benefit.

- Patients occupying shared areas of hospitals (such as multi-bed wards) have the right to expect privacy and they should be offered an opportunity when speaking to hospital staff to move to a more private space. A private consultation room should be made available in all cases which offers patients an adequate level of speech privacy.

# Absence of Audit Trails

## Context

Every year hundreds of thousands of patients attend acute hospitals in the State. For every patient who attends at a hospital a record, which contains basic demographic details, is created on an electronic patient administration system at the hospital concerned.  Hospitals, therefore, create thousands of patient electronic records annually. Securing the personal data contained in these records requires, among other things, measures such as functioning audit trails, as well as effective monitoring of those audit trails, to guard against unauthorised access.

All hospitals inspected use various electronic database systems for patient administration and a range of other purposes such as clinical records management regarding radiology, scans, etc. Many database management systems that operate in the modern world of technology include an audit trail (or audit log) component. In simple terms, an audit trail is a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. A robust audit trail function should have the capacity to record 'read-only' access (where the user accessed the record but made no amendments or additions to it) as well as 'edit' access (where the user amended or added information to the record). Audit trails are, therefore, an essential and very useful tool for maintaining the security and integrity of an electronic database system.

While all hospitals inspected had an audit trail component on their electronic database systems that had the capability to record 'edit' access, in the majority of cases the systems in use in many hospitals for patient administration purposes, in particular, had no functioning 'read-only' access audit trail functionality. Some hospitals are in the process of upgrading the current version of their patient administration system. However, in some instances, the upgraded version continues to have no 'read-only' audit trail functionality or the functionality is not activated because of fears that it might slow down the patient administration system overall.

An electronic case management system, known as the Maternity & Newborn Clinical Management System (MNCMS) is currently being rolled out in maternity hospitals and in acute hospitals that provide maternity services across the State. A total of nineteen hospitals provide maternity services in Ireland and MNCMS has been rolled out in a small number of those hospitals to date. In one of the hospitals inspected where MNCMS is in operation it was noted that while the auditing functionality was activated the hospital staff did not have local access to the auditing functionality or the ability to generate auditing reports.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

The key risks that can be identified where fully functioning audit trails (i.e. including 'read-only' access) are not in place include accesses by snooping staff and accesses arising from 'blagging.' Such accesses, which constitute data security breaches, may go undetected in the absence of fully functioning audit trails. On the basis of the inspections carried out, access by staff to electronic patient records currently lacks sufficient monitoring in some hospitals.

*Recommendations*

- A robust audit trail component that captures both 'read-only' and 'edit' accesses should be implemented on all electronic patient record databases. Any technical issues which currently impede the implementation of this recommendation must be resolved without delay as such technical issues should not outweigh the data protection considerations in this key matter.

- The audit trail output should be monitored on a regular basis to detect if any unauthorised accesses or failed attempts to log in to patient records are occurring.

- Rigid procedures should be implemented to ensure that access rights to electronic patient records are confined to those staff who require access on a 'need to know' basis to specific patient records in line with their job role and the care and treatment of the patient. Appropriate controls should be put in place to ensure that those procedures are followed. In short, no medical, clinical or nursing staff should be given unrestricted access to all electronic patient records irrespective of whether or not they have a business need to have such access.

- To deter staff from accessing electronic patient records without a business reason for doing so, hospitals should devise policies that treat such unauthorised accesses as a disciplinary matter.

### Risk No. 2

The MNCMS holds a significant amount of personal data and sensitive personal data in relation to mothers and their babies including demographics, health records and clinical data. The absence of pro-active monitoring of the audit trail of accesses to data held on this electronic system poses the risk of undetected unauthorised access.

#### *Recommendation*

- All hospitals that provide maternity services and in which MNCMS is currently in use or will in the future be used should ensure that they have access to, and that staff are fully trained on the use of, P2 Sentinal which is the auditing tool for this system. The audit trail output should be monitored on a regular basis to detect if any unauthorised accesses are occurring.

# Raising Awareness of Data Protection in Hospitals and the Provision of Data Protection Information to Patients

## Context

Practices vary greatly across the hospitals inspected both in relation to providing information to patients about how their personal data will be used and in relation to notifying patients of a contact point in the event that any data protection concerns arise while they are attending the hospital. Likewise, efforts to inculcate an awareness of data protection amongst hospital staff on an ongoing basis differ significantly in the hospitals inspected.

Many hospitals have information notices of varying sizes and varying content on display in some public areas such as reception and waiting zones. Some such information notices refer briefly to the hospital's commitment to privacy or data protection. Some hospitals also provide patients with information leaflets or booklets that cover numerous topics of interest to admitted patients, including privacy and data protection. In a small number of hospitals inspected, notices were on display in staff areas reminding staff of their obligations with regard to patient confidentiality and data protection. In some, but not all hospitals inspected, data protection training was mandatory. One hospital facility had rolled out a programme of data protection 'champions' from within its staff to promote data protection awareness. On the other side of the scale, a different hospital had no nominated staff members assigned to handle data protection matters.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

From the time of arrival to the subsequent point of discharge, however long that may be, a patient's hospital attendance experience results in a whole range of personal and sensitive personal data processing operations. Behind every hospital attendance is the creation and processing of patient registration forms, charts, scans and other documentation containing personal data and sensitive personal data. Hospitals, as data controllers, are obliged to inform patients about how their data will be used and for what purpose. Failure to so inform patients breaches the principle of fair processing and transparency.

### *Recommendation*

- Comprehensive information set out in an easy-to-read format should be made available to patients who attend hospital and to other members of the public (such as visitors or next-of-kin) whose personal data may be processed by hospitals. This information should explain in plain language how the hospital will process personal data and sensitive personal data and for what purpose it will be processed. This information may be made available in the format of information leaflets, information posters displayed in key areas, hospital websites, etc. All such information notices should include the name and contact details of a hospital staff member who has been assigned responsibility for handling data protection concerns that patients or others may wish to raise.

## Risk No. 2

The importance of data protection and patient confidentiality must permeate the hospital culture at all times. Failure to maintain a high level of staff awareness amongst all staff of data protection and patient confidentiality poses the significant risk that staff may let their guard down and disclose personal data or sensitive personal data to third parties either inadvertently or intentionally.

One particular note of concern that arose during the inspections related to staff who were operating reception desks. For example, it was observed in some cases that attending patients presented a referral letter or a letter of appointment at reception desks. In some instances, the receptionist proceeded to call out to the attending patient the personal details contained on the letter in the expectation of a ‘Yes’ or ‘No’ reply as a means of confirming the patient’s identity and personal data. Apart from the fact that these details could be overheard, the inspectors were concerned about the manner in which, in these circumstances, patients were requested to confirm details of their personal data rather than being asked directly to provide their personal data. The hospital concerned admitted that staff had not been trained to confirm personal data on the basis of a 'Yes' or 'No' reply and it recognised the potential that inaccurate personal data might be captured.

### *Recommendations*

- Staff training programmes on data protection should be reviewed to ensure that they include periodic refresher training for all staff to remind them of their obligations in relation to respecting the data protection rights of patients.

- Training programmes for reception staff should be rolled out on a regular basis to ensure that best practices for the capture of personal data are observed and implemented at all times.

- Notices should be displayed prominently in staffing areas of hospitals such as offices, meeting rooms, staff canteens, etc to continually highlight to hospital staff their obligations in relation to respecting the data protection rights of patients. This should form part of an overall drive by hospitals to foster among staff a culture that places the confidentiality of patient information at the forefront of their minds at all times.

## Risk No. 3

In some instances, the inspectors noted that patient records stored on the electronic patient information system operating in a hospital may be accessible to several other hospitals in the same geographical region. In those circumstances, patients are not made aware that their personal data may be shared with other hospital facilities in the same geographical region – in some instances with different data controllers. Furthermore, the inspectors noted in one hospital the practice of transferring the patient's chart with the transferred patient to a specialist hospital in the same region without notifying the patient or obtaining their consent. There is a significant risk of personal data disclosure from one data controller to another without a legal basis for doing so in such instances if the patient has not been informed of or consented to the data transfer.

*Recommendations*

- Where patient data held on patient information systems is accessible to other hospital facilities in the same geographical region, patients must be informed accordingly by means of patient information leaflets given to each patient and the legal basis for such data sharing should be clarified.

- Where hospitals need to share personal or sensitive personal data with other hospital facilities during the course of a patient's care or treatment, the patients concerned should be made aware of the necessity for such data sharing and be given the opportunity to consent to it.

# Consent for Research

## Context

The Data Protection Commissioner published a substantial guidance document entitled “Data Protection Guidelines on Research in the Health Sector” in November 2007 that outlined a basis on which research and clinical audit in the health area may be carried out in a manner consistent with the framework of data protection legislation.

During the course of the hospital inspections undertaken last year, our inspectors uncovered a practice in one hospital where medical staff such as nurses or doctors were permitted to examine patient charts for their own research purposes, such as the completion of their medical studies (as distinct from research for the purposes of a project approved by the hospital’s Ethics Committee). The inspectors noted that the consent of the patients concerned was not sought for such research.

When the GDPR comes into effect on 25 May, 2018 the conditions for consent as laid down in Article 7 will apply. The onus will lie on data controllers to ensure that if a data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The data subject shall have the right to withdraw his or her consent at any time and they shall be advised accordingly prior to giving consent. Furthermore, it shall be as easy to withdraw consent as to give it.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

Hospital patients have a reasonable expectation that their health information will be kept confidential and that it will not be used for a purpose beyond their care and treatment by medical staff who are not involved in their care. Permitting medical staff to have access to patient charts or other patient information for the purposes of research for their own studies is a form of further processing beyond the purposes for which the data was obtained. This requires specific consent of the patient as well as safeguards for the data while it is in the possession of the staff concerned.

### *Recommendations*

- All hospitals should review current practices in relation to obtaining patient consent for research and clinical audit to ensure that they follow the guidelines published by the Data Protection Commissioner in November 2007.

- Any existing or ongoing practices that permit hospital staff to access patient charts or other patient information for the purposes of medical studies should be identified and appropriate steps should be taken to ensure that patient data is not being accessed or otherwise used in those circumstances without the knowledge and consent of the patients concerned.

- In all cases where patient data is made available to staff for research and where patient consent is obtained, hospitals should ensure that appropriate safeguards are in place to protect the data and to ensure that it is kept in a safe environment within the hospital at all times.

# The Processing of Private Health Insurance Information in Hospitals

## Context

Several issues of concern came to light over the course of the hospital inspections in relation to the processing of information concerning private health insurance.

Some hospitals seek health insurance details from all patients who have such cover at the point of attendance at the Emergency Department, even though the patient may not subsequently be admitted (it is at the point of admission that insurance cover normally takes effect).

Some health insurance companies carry out on-site audits at hospitals to assist in the assessment and verification of health insurance claims. Normally during the course of their admission patients are given the opportunity by hospitals to consent to the sharing of their information in relation to the particular hospital attendance with their health insurance provider for the purposes of processing their health insurance claim in respect of that particular admission and treatment. In the course of the inspections, it was noted in some instances that during the course of on-site audits by insurance companies, some hospitals allowed the auditors access to the patient's complete medical chart, even though some of the records on the chart related to previous attendances that were not the subject of the claim being audited. Furthermore, practices in hospitals concerning the supervision of health insurance company auditors while they were reviewing patient charts differed widely with some hospitals allowing auditors a free rein to review charts without any hospital supervision.

The main health insurance companies in Ireland each provide hospitals with a portal or patient verification system by which staff in hospital finance units can verify a patient's insurance cover. One issue of concern noted in the inspections was the practice in some hospitals of permitting hospital staff to log on to a health insurance portal under one user name.

A second issue of concern is the noted practice in some hospitals of staff accessing the health insurance portals, particularly in advance of a patient's scheduled appointment, to check their level of insurance cover. This is done without the knowledge or consent of the patient – who may have no intention of making a claim on their health insurance policy.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

Any practices of seeking details of health insurance cover at the point of the patient's registration at the Emergency Department poses the risk of excessive processing of personal data. As attendance and treatment at an Emergency Department is generally not covered under health insurance policies, and as there is a high rate of discharge of patients following their attendance at an Emergency Department, any collection of the health insurance details of such discharged patients is unnecessary and, therefore, constitutes excessive data processing.

#### *Recommendation*

- Private health insurance information should only be sought from patients whose hospital attendance will be the subject of a claim on their health insurance policy.

### Risk No. 2

Data protection legislation does not stand in the way of very legitimate auditing of insurance claims submitted by patients where those patients have consented to their personal and sensitive information being shared with or made available to their health insurers. However, the creation and subsequent building of a patient's hospital chart, often over a period of many years and several instances of attendances, is done by reference to attendance and not by reference to health insurance claims. Potentially, a patient's hospital chart may include several attendances over a long period, some of which may not have been the subject of a health insurance policy claim or which may have been the subject of a health insurance claim with a different health insurance provider. Given the potential vast scope of material on a patient's medical chart, it stands to reason that allowing an auditor from a health insurance company unrestricted or unsupervised access to a full medical chart, poses the high risk that the auditor may access patient information which is not the subject of the extant claim.

*Recommendations*

- Access controls for health insurance company auditors who seek access to patient charts or other patient information, either on-site or otherwise, should be reviewed to ensure that strict controls are in place that restrict access to the relevant patient records in line with the consent provided by the patient at the time of attendance.

- For the purpose of on-site inspections of patient charts or other records by health insurance company auditors, the supervising role of hospital staff in relation to such auditors should be reviewed to ensure that such hospital staff have sufficient authority to guard against excessive accessing of data held on patient charts by health insurance auditors.

### Risk No. 3

Access to the health insurance portals or patient verification systems by hospital staff must be capable of complete auditing in terms of the records of who accessed the records and when they did so. Any logging on to a health insurance portal by staff under one user name renders that audit function meaningless and exposes to unauthorised access the personal data that is accessible on the portal.

*Recommendation*

- Strict protocols should operate in all hospitals that have been supplied with health insurance portals to ensure that all staff who have access rights to those portals must log on individually rather than by means of logging on under one user name.

## Risk No. 4

The provision of portals or patient verification systems to hospitals by the health insurance companies is to facilitate the finance units of hospitals in relation to processing claims that the patients concerned have decided to lodge in respect of their attendance and/or treatment. It is entirely a matter for an insured patient to decide whether or not to lodge a health insurance claim, to attend the hospital as a public patient (if that is an option) or to pay the hospital fees from their own resources. Any delving into the information held on the health insurance portals by hospitals to determine whether a patient or prospective patient has health insurance cover or the level of that cover, when the patient has not informed the hospital that he/she intends to make a claim on their health insurance policy, can be deemed to breach the principles of fair obtaining and fair processing.

### *Recommendation*

- Strict protocols should operate in all hospitals that have been supplied with health insurance portals to ensure that staff do not access the health insurance information of any patient who has not informed the hospital of their health insurance details or has not consented to having their hospital attendance fees discharged by means of a claim on their health insurance policy.

# Maternity Service Users

## Context

Maternity services are provided in nineteen hospitals in the State. Some of these hospitals are dedicated maternity hospitals while in the majority of cases maternity services are provided alongside numerous other disciplines of care at acute hospitals. One main issue of concern arose in relation to maternity services users (pregnant women) in some of the hospitals inspected.

A chart called the National Maternity Healthcare Record is created for each expectant mother at their first ante natal clinic. In some hospitals, custody of this chart is given to the expectant mother at this point and she is required to bring it with her each time she attends the hospital for an ante natal appointment and when she presents for delivery. The expectant mother also brings this chart to any pregnancy-related appointments that she may have with her GP during the course of her pregnancy. The National Maternity Healthcare Record that is contained in the chart consists of a substantial amount of both personal and sensitive personal data. Of particular note in that regard is the Antenatal Outpatients section of the chart that contains information on the expectant mother's medical history, obstetric history and risk factors assessment.

## Risks Identified and Recommendations to Mitigate the Risks

### Risk No. 1

Given the sensitivity of some of the personal information that may be held on the National Maternity Healthcare Record, it is imperative that expectant mothers are allowed to choose whether or not to take custody of the chart for the duration of their pregnancy. Personal data and sensitive personal data contained in the National Maternity Healthcare Record may be exposed to inappropriate access by third parties while the chart is in the possession of the expectant mother. In certain situations, domestic or otherwise, such exposure of their private and very sensitive medical information could have serious negative consequences for the expectant mother.

### *Recommendations*

- Expectant mothers should be given the option to choose whether or not to accept custody of their National Maternity Healthcare Record for the duration of their pregnancy.

- Hospital staff should be fully trained in relation to the process of giving expectant mothers the option to choose whether or not to accept custody of their National Maternity Healthcare Record. In that regard, staff must be trained to fully recognise and appreciate the sensitivity of personal data that may be included in such Records. They must be capable of fully informing and warning expectant mothers of the sensitivities concerned and they must be able to advise them of the care that must be taken in relation to the safe-keeping of the Record while it is in their custody.

- Hospitals must implement a robust procedure to ensure that all National Maternity Healthcare Records are returned to the hospital concerned following delivery.

# Data Retention

## Context

Data controllers must comply with the obligation contained in Section 2(1)(c) of The Acts that *"personal data shall not be kept for longer than is necessary for that purpose or those purposes [for which it was obtained]"*. When the GDPR comes into force from 25 May, 2018 the obligations set down in Article 3(1)(c) will apply: *"personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."* In effect these provisions mean that a data controller shall not retain personal data indefinitely. It is a matter for each data controller to determine the retention periods that apply to every category of personal data that it holds. Having determined the retention periods, the data controller must implement processes to safely dispose of the personal data once the retention periods have been reached.

In 2013 the Health Service Executive published its policy document on Record Retention Periods. This policy updated the 1999 Health Board retention policy. The policy includes defined retention periods for records and systematic disposal of records within a reasonable period after the retention period expires. The policy document sets out four distinct categories of records: Healthcare Records, Environmental Health Records, Personnel/HR Records and Financial Records.

According to the HSE policy document, the final action in respect of most healthcare records where the retention period has been reached is *"destroy under confidential conditions."* The document sets out a range of differing retention periods for different types of healthcare records. Basic healthcare records in the form of hospital charts are given a retention period of *"8 years after conclusion of treatment or death."*

In the course of the hospital inspections carried out in 2017, the majority of hospitals inspected retained patient charts indefinitely, irrespective of whether the patient's treatment had concluded for a period longer than the retention period and irrespective of whether the patient was now deceased. In short, while the majority of hospitals have adopted the HSE policy in relation to data retention periods, there is little evidence that processes have been put in place to give effect to the policy by means of an effective data destruction programme, hence the widespread practice of retaining patient charts indefinitely.

## Risk Identified and Recommendations to Mitigate the Risk

### Risk No. 1

Retaining personal data or sensitive personal data for indefinite periods contravenes the principles set down in the current data protection legislation and it will contravene the principles set down in the GDPR when it comes into effect. As well as the risk of contravening those principles, there are other risks associated with keeping records indefinitely. In particular, the safe keeping and storage of records presents significant challenges and costs. Furthermore, once records are kept by a data controller, a data subject has a statutory entitlement to get access to them both under data protection and freedom of information legislation. In relation to archived records in particular, therefore, a real risk emerges that access requests may not be complied with in full where the data controller fails, in processing access requests, to take into account patient charts and other patient information that may be in off-site storage.

*Recommendations*

- Hospitals that are not currently implementing a procedure to safely destroy patient information once their data retention policy's retention period is reached, should carry out an internal analysis and review to establish the cause of this situation.

- Once the cause of the situation has been established, the hospital should take proactive steps to remedy the situation including, if necessary, the revision of the retention periods set down in its data retention policy and the implementation of workable processes that provide for the safe destruction, on an annual basis at a minimum, of patient data that has reached its retention period.

# EXECUTIVE SUMMARY

## Background

In 2017, as part of a special investigation, Authorised Officers of the Data Protection Commissioner carried out inspections at twenty hospitals across the State spanning HSE facilities, voluntary hospitals and private hospitals. The investigation examined the processing of patient sensitive personal data in departments and areas of hospitals to which patients and the public have access. It concentrated, as far as possible, on the circulation and journey of patient charts and medical files in order to identify if there were any shortcomings in terms of meeting the requirements of the Data Protection Acts, 1988 & 2003 ['The Acts'] to keep personal data safe and secure and to have appropriate measures in place to prevent unauthorised access to or disclosure of personal data.

Based on the findings of the investigation and where issues of concern were identified with regard to data protection compliance, the aim of the investigation was to make recommendations for improvements with regard to the processing of patient sensitive personal data not only in the hospitals which were selected to participate in the investigation but across the Hospitals Sector in general.

This report, therefore, takes account of the findings of the twenty inspections undertaken last year. In many of the hospitals inspected, our inspection teams encountered similar matters of concern arising. The Data Protection Commissioner considers that the contents of this report will be of significant value to hospitals that were not part of the inspection process. The Commissioner expects that all hospitals will identify with some, if not several, of the matters of concern that are outlined in this report and that they will find the recommendations that we make in this report to be a useful guide towards mitigating the identified risks.

## Matters of Concern

This report sets out fourteen main matters of concern that arose from our hospital inspections in 2017. These matters of concern are summarised as follows:

## Controls in Medical Records Libraries

Medical Records Libraries provide a critical and essential function with regard to the safe-keeping of physical patient charts. Usually these Libraries are located in a part of the hospital facility to which patients or other members of the public do not have access. Overall, the inspectors found that there is scope for much greater security controls with regard to Medical Records Libraries in light of the fact that physical patient charts contain the most detailed clinical records in relation to the patient's care, condition and treatment at the hospital.

This report identifies six risks in relation to controls in Medical Records Libraries and it sets out thirteen recommendations to mitigate those risks. The risks identified were as follows:

- In some instances, controls were lax with regard to restricting access to the Medical Records Library by hospital staff who are employed in other parts of the hospital. Any deficit in restricting access to the Medical Records Library by staff who have no ongoing business need to enter that area poses the very serious potential risk that staff members could enter the Library to snoop through medical charts of family members, friends or others out of sheer nosiness or for other more sinister purposes.
- Only a small number of the inspected hospitals have a means to record staff access to their Medical Records Libraries. The remainder had no means of monitoring unauthorised staff access. Unmonitored access to the Library area of a hospital containing the most sensitive personal data of thousands of patients lends itself to a high risk of unauthorised access by staff who have no business reason to enter the area.
- Practices varied in the hospitals inspected with regard to 'after-hours' staff access and accountability for charts removed from the Medical Records Library during 'after-hours' periods. In many cases, no logs were created to record details of who entered the Library or details of which chart they removed. There was little evidence of any restriction on a staff member who has access to the Library 'after-hours' from bringing an 'unauthorised' staff member to the Library with them.

- The Medical Records Library in most hospitals inspected had no alert system in place to draw attention to charts which had been previously removed from, but not been returned to, the Library by a certain period of time.
- Open top trolleys (on four wheels) are commonly used to transport patient charts from the Medical Records Library to the various hospital departments where they are required. Patient charts that are transported in an open-top trolley from the Library to another location of the hospital via corridors, lifts and wards are particularly vulnerable to exposure. In a busy public area of a hospital, there is a high risk that the staff member in control of the trolley could become distracted or otherwise engaged, thus bringing the security of the patient charts into question.
- In some hospitals inspected, there was no electronic tracking of chart movement. Instead, the monitoring of chart movement was based solely on a manual system of updating a tracer card in the Medical Records Library. In one instance, updates to the tracer card were triggered by telephone calls to the Medical Records Library from staff involved in the movement of the chart in the various hospital departments. Such a manually operated system presents a significant risk that chart tracking may not be up-to-date with the added risk that if a chart is required urgently, its current location may not be readily identifiable.

## Security

In general, rigid controls are in place in hospitals to restrict public access to certain parts of hospital facilities. However, some concerns were noted during the course of the hospital inspections in relation to security features on computer workstations, and in relation to the handling and storage of patient charts and other forms of patient information.

This report identifies eight risks in relation to security and it sets out twenty three recommendations to mitigate those risks. The risks identified were as follows:

- Some inspections found areas of weakness in relation to access controls on some doors leading to restricted areas and in relation to wide-ranging levels of swipe card access for staff. Weaknesses in relation to the security of doors has the potential to jeopardise the safe-keeping of patient charts that may be stored in the affected areas and thereby put personal data and sensitive personal data at risk of unauthorised access.

- In a number of instances, personal data on computer screens was viewable by passers-by due in the main to the physical positioning of the computer screen.
- In other instances, a lack of appropriate technical safeguards resulted in unattended computer screens remaining open for lengthy periods of inactivity thereby exposing the personal data on the open screens to being viewed by passers-by. In addition, instances of staff failing to log off after use could result in the next user inputting information using the previous user's account.
- In relation to the handling and storage of patient data, risks identified included the storage of patient charts in unsecure filing cabinets; the storage of emergency department cards ('ED' cards) in Emergency Departments for indefinite periods; the storage of keys of filing cabinets used for the filing of patient charts or files in insecure locations; the use of see-through plastic holders mounted on walls to store patient information; the leaving of patient charts on shelves or tables outside of consultation rooms in Outpatient Departments or on counter-tops in various hospital reception areas; and the leaving of confidential correspondence in unattended areas.
- The practice of requiring patients who check-in to hospital via an Admissions Office to carry their medical chart to the ward to which they are assigned presents a risk to the safety of the chart while it is in the custody of the patient.
- There is a potential risk that some hospitals may not have data security breach protocols in place and on time to comply with legal obligations under Articles 33 and 34 of the GDPR when it comes into effect on 25 May, 2018.
- In one hospital inspected, concerns arose about items of incoming and outgoing postal correspondence that, as standard practice, were left in unsecured wire trays in an unprotected environment while awaiting collection by hospital porters. There was a high risk that the personal and sensitive personal data of patients that was contained in the postal correspondence could easily be inappropriately accessed by patients or visitors. In another instance, postal correspondence was left in an open unsecured tray

on a counter top in a public ward where passers-by could easily access it.

- Almost all hospitals inspected use third party service providers for the storage of physical medical charts that have reached a certain age. In one hospital inspected, confusion arose in relation to whether or not a contract was in place with the off-site storage service provider.

### Storage of Patient Observation Charts in Hospital Ward Settings

Most patient observation charts are used to monitor, at a minimum, the patient's vital signs such as body temperature, heart rate or pulse, respiratory rate and blood pressure. Usually the patient's full name and date of birth are recorded on the observation chart. This report identifies one risk with regard to the storage of patient observation charts in hospital ward settings and it sets out two recommendations to mitigate that risk. The following risk was identified:

- In some of the hospital facilities inspected, as standard practice, patient observation charts in respect of admitted patients are clipped to the end of each patient's bed. Where the patient is admitted to an isolation ward, it is standard practice in some hospital facilities to hang the patient's observation chart on a wall rail immediately outside of the patient's isolation ward, usually in a corridor area. In both of these situations, as the observation charts are unprotected and unsecured there is a high risk that the observation charts of patients could be viewed or accessed inappropriately by third parties such as other patients, visitors or other members of the public. These practices lend themselves to situations whereby the personal data of patients is exposed to snooping third parties, such as visitors in particular.

## Storage of Patient Charts in Trolley Bins in Ward Settings

A Healthcare Record, commonly known as a Patient Chart, is normally created for every admitted patient in hospitals across the State. This report identifies two risks in relation to the storage of patient charts in trolley bins in ward settings and it sets out three recommendations to mitigate those risks. The risks identified were as follows:

- In the ward setting of some of the hospitals inspected, patient charts of the current admitted patients are stored in what are known as chart trolley bins. Of particular concern, were situations where unlocked trolley bins were parked outside of the Nurses' Station where the patient charts within them could potentially be accessed by passers-by such as patients, visitors or other members of the public.
- In some hospitals, the inspectors noted instances where patient charts were stored in an unprotected environment in the open shelving space at the bottom of the trolley bins or in hanging devices at the side of trolley bins.

## Storage of Confidential Waste Paper Within the Hospital Setting

Given the nature of the work carried out in a hospital environment, it follows that much of the confidential waste generated relates to patients in terms of personal information relating to their medical condition, treatment, health insurance, medical appointments, etc. This report identifies one risk with regard to the storage of confidential waste paper within the hospital setting and it sets out one recommendation to mitigate that risk. The following risk was identified:

- Several hospitals that were inspected use paper bins, bags or trays that are not secure in offices, sections and wards throughout the facility. Typically, in these situations, waste paper that is placed in these bins, bags or trays can be removed by others.

## Disposal of Handover Lists and Patient Lists

In ward settings of several, but not all, hospitals inspected nursing staff carry physical paper ‘handover lists’ or ‘patient lists’ in the pockets of their uniforms for the duration of their shift. This report identifies one risk with regard to the disposal of handover lists and patient lists and it sets out two recommendations to mitigate that risk. The following risk was identified:

- The inspectors found no evidence that any of the hospitals that use such lists monitor compliance with the standard procedure for accounting for the disposal of those lists. In the absence of an end-of-shift procedure to account for the secure disposal of such lists, there is a significant risk that nursing staff may inadvertently take the lists out of the hospital setting at the end of their shift and dispose of them at a later point elsewhere.

## Use of Fax Machines

The level of fax machine usage remains high in hospitals despite the availability of encrypted email as a more secure method of electronic communication. This report identifies two risks with regard to the use of fax machines and it sets out two recommendations to mitigate those risks. The following risks were identified:

- One of the biggest risks associated with the use of fax machines is human error when dialling the number to send an outgoing fax message. Particular risks arise around dialling the digits in the correct order as well as omitting to dial or incorrectly dialling the area code of the receiving fax number.
- The inspectors noted of lack of guidance for fax machine users in many hospitals to inform them of best practice with regard to the sending or receiving of fax messages containing sensitive personal data.

## Lack of Speech Privacy

Speech privacy is achieved when speech, or conversations between two or more parties, cannot be understood by other individuals who may be in close proximity. One of the most common matters of concern noted in the hospital inspections was the lack of speech privacy in various areas of hospital facilities. This report identifies two risks with regard to the lack of speech privacy and it sets out six recommendations to mitigate those risks. The following risks were identified:

- In those areas of hospitals where the inspectors noted a lack of speech privacy, there existed a real potential for third parties such as other patients and hospital visitors, to over-hear private conversations between patients and hospital staff. This was particularly notable at reception desks where patients orally provide several elements of their personal data to hospital staff.
- Another striking example of the lack of speech privacy noted by the inspectors occurred in the treatment cubicles of some Emergency Departments. Private conversations taking place in these cubicles between medical staff and patients could easily be overheard in the adjoining cubicles at either side. Discussions of a most sensitive nature take place between medical staff and patients in treatment cubicles of Emergency Departments around matters such as symptoms, previous medical history, treatment plans, etc.

## Absence of Audit Trails

For every patient who attends at a hospital a record, which contains basic demographic details, is created on an electronic patient administration system at the hospital concerned. Securing the personal data contained in these records requires, among other things, measures such as functioning audit trails, as well as effective monitoring of those audit trails, to guard against unauthorised access. While all hospitals inspected had an audit trail component on their electronic database systems that had the capability to record ‘edit’ access, in most cases the systems in use in many hospitals for patient administration purposes, in particular, had no functioning ‘read-only’ access audit trail functionality.

This report identifies two risks with regard to the absence of audit trails and it sets out five recommendations to mitigate those risks. The following risks were identified:

- Accesses by snooping staff and accesses arising from 'blagging' may go undetected in the absence of fully functioning audit trails on electronic patient administration systems. On the basis of the inspections carried out, access by staff to electronic patient records currently lacks sufficient monitoring in some hospitals.
- The Maternity & Newborn Clinical Management System (MNCMS) which is currently being rolled out in hospitals that provide maternity services holds a significant amount of personal data and sensitive personal data in relation to mothers and their babies including demographics, health records and clinical data. The absence of pro-active monitoring of the audit trail of accesses to data held on this electronic system poses the risk of undetected unauthorised access.

## Raising Awareness of Data Protection in Hospitals and the Provision of Data Protection Information to Patients

Many hospitals have information notices of varying sizes and varying content on display in some public areas such as reception and waiting zones. Some such information notices refer briefly to the hospital's commitment to privacy or data protection. Some hospitals also provide patients with information leaflets or booklets that cover numerous topics of interest to admitted patients, including privacy and data protection. This report identifies three risks with regard to the lack of awareness raising of data protection in hospitals and in the provision of data protection information to patients and it sets out six recommendations to mitigate those risks. The following risks were identified:

- Behind every hospital attendance is the creation and processing of patient registration forms, charts, scans and other documentation containing personal and sensitive personal data. Hospitals, as data controllers, are obliged to inform patients about how their data will be used and for what purpose. Failure to so inform patients breaches the principle of fair processing and transparency.

- Failure to maintain a high level of staff awareness of data protection and patient confidentiality poses the significant risk that staff may let their guard down and disclose personal data or sensitive personal data to third parties either inadvertently or intentionally.
- In some instances, the inspectors noted that patient records stored on the electronic patient information system operating in a hospital may be accessible to several other hospitals in the same geographical region. In those circumstances, patients are not made aware that their personal data may be shared with other hospital facilities in the same geographical region – in some instances with different data controllers. Furthermore, the inspectors noted in one hospital the practice of transferring the patient's chart with the transferred patient to a specialist hospital in the same region without notifying the patient or obtaining their consent. There is a significant risk of personal data disclosure from one data controller to another without a legal basis for doing so in such instances if the patient has not been informed of or consented to the data transfer.

## Consent for Research

Our inspectors uncovered a practice in one hospital where medical staff such as nurses or doctors were permitted to examine patient charts for their own research purposes, such as the completion of their medical studies (as distinct from research for the purposes of a project approved by the hospital's Ethics Committee). The inspectors noted that the consent of the patients concerned was not sought for such research. This report identifies one risk with regard to research conducted without patient consent and it sets out three recommendations to mitigate that risk. The following risk was identified:

- Permitting medical staff to have access to patient charts or other patient information for the purposes of research for their own studies is a form of further processing beyond the purposes for which the data was obtained. This requires specific consent of the patient as well as safeguards for the data while it is in the possession of the staff concerned.

## The Processing of Private Health Insurance Information in Hospitals

This report identifies four risks with regard to the processing of private health insurance information in hospitals and it sets out five recommendations to mitigate those risks. The following risks were identified:

- The practice of seeking details of health insurance cover at the point of the patient's registration at the Emergency Department poses the risk of excessive processing of personal data. As attendance and treatment at an Emergency Department is generally not covered under health insurance policies, and as there is a high rate of discharge of patients following their attendance at an Emergency Department, any collection of the health insurance details of such discharged patients is unnecessary and, therefore, constitutes excessive data processing.
- Potentially, a patient's hospital chart may include several attendances over a long period, some of which may not have been the subject of a health insurance policy claim or which may have been the subject of a health insurance claim with a different health insurance provider. Given the potential vast scope of material on a patient's medical chart, it stands to reason that allowing an auditor from a health insurance company unrestricted or unsupervised access to a full medical chart, poses the high risk that the auditor may access patient information which is not the subject of the extant claim.
- Access to the health insurance portals or patient verification systems by hospital staff must be capable of complete auditing in terms of the records of who accessed the records and when they did so. Any logging on to a health insurance portal by staff under one user name renders that audit function meaningless and exposes to unauthorised access the personal data that is accessible on the portal.
- Any delving into the information held on the health insurance portals by hospitals to determine whether a patient or prospective patient has health insurance cover or the level of that cover, when the patient has not informed the hospital that he/she intends to make a claim on their health insurance policy, can be deemed to breach the principles of fair obtaining and fair processing.

## Maternity Service Users

One matter of concern arose in relation to maternity services users (pregnant women) in some of the hospitals inspected. It relates to the National Maternity Healthcare Record which is a chart that is created for each expectant mother at their first ante natal clinic. In some hospitals, custody of this chart is given to the expectant mother at this point and she is required to bring it with her each time she attends the hospital for an ante natal appointment and when she presents for delivery. This report identifies one risk with regard to custody of the National Maternity Healthcare Record and it sets out three recommendations to mitigate that risk. The following risk was identified:

- Given the sensitivity of some of the personal information that may be held on the National Maternity Healthcare Record, it is imperative that expectant mothers are allowed to choose whether or not to take custody of the chart for the duration of their pregnancy. Personal data and sensitive personal data contained in the National Maternity Healthcare Record may be exposed to inappropriate access by third parties while the chart is in the possession of the expectant mother.

## Data Retention

The majority of hospitals inspected retained patient charts indefinitely, irrespective of whether the patient's treatment had concluded for a period longer than the retention period and irrespective of whether the patient was now deceased. In short, while the majority of hospitals have adopted the HSE policy in relation to data retention periods, there is little evidence that processes have been put in place to give effect to the policy by means of an effective data destruction programme, hence the widespread practice of retaining patient charts indefinitely. This report identifies one risk with regard to data retention in the context of patient charts and it sets out two recommendations to mitigate that risk. The following risk was identified:

- Retaining personal data or sensitive personal data for indefinite periods contravenes the principles set down in the current data protection legislation and it will contravene the principles set down in the GDPR when it comes into effect. As well as the risk of contravening those principles, there are other risks associated with keeping records indefinitely. In particular, the safe keeping and storage of records presents significant challenges and costs. Furthermore, once records are kept by a data controller, a data subject has a statutory entitlement to get access to them both under data protection and freedom of information legislation. In relation to archived records in particular, therefore, a real risk emerges that access requests may not be complied with in full where the data controller fails, in processing access requests, to take into account patient charts and other patient information that may be in off-site storage.

# Conclusion

In examining whether any or all of the matters of concern are occurring or could occur in its facility, each hospital is advised to consider every part of the entire hospital campus as part of its examination in order to establish the relevancy, if any, of each of the risks and recommendations in each area. The implementation of the recommendations will not be achieved by simply issuing reminders to staff or by creating standard operating procedures. Rather, it will be necessary for each hospital to support the implementation of the recommendations by putting in place the necessary infrastructure and resources that may be required as essential enablers.

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

May 2018