

New Legal Issues in E-Health Practices

1. Introduction: What Is E-Health?

The term *e-health* was coined in the United States to refer to health care delivered to patients remotely using telecommunications and computer-based information systems.

The practice originated in the 1970s with the need to provide astronauts with clinical care and first aid in real time in the course of a space flight.

At the core of e-health is health care proper, such as telediagnosis and telerobotic surgery. Yet e-health is much broader than that and also covers any use of telecommunications to provide medical services generally: it thus includes communicating clinical test results at a distance for a second opinion (tele-consultation), sharing clinical

information among medical specialists for the purpose of diagnosis, and using practice-management systems to schedule appointments and access electronic health records, which store patient data (including text, charts, graphs, and images) that travels for the patient instead of the patient traveling for it.

We can see, then, how e-health—at first a circumscribed practice—has grown to impressive proportions and caused us to rethink our way of delivering health care and to redesign the healthcare system accordingly.¹

There are no doubt great advantages that e-health can afford in providing health care, especially home care for the elderly, the physically impaired, and the chronically ill (patients with heart disease, asthma, diabetes). Indeed, e-health uses not just the phone line to send biomedical data to a general or a specialized hospital, but also high-speed Internet

¹ L. Mazzei, “La Telemedicina: Prospettive ed aspetti critici,” Centro Studi Assobiomedica, Milan, Issue No. 11, March 2005.

connections so that a hospital can receive radiographs in a digital format at full resolution.

The family doctor plays a strategic role here as the main online liaison, using the Internet to communicate clinical test results to patients and making for faster access to diagnoses and to prescriptions for therapies.

E-health thus greatly benefits patients by making medical services available to them in real time, which means that waiting periods are cut down and more time is available for actual therapy.²

Health protection figures among the main objectives of EU policy, and as the European Commission pointed out in a 2007 communication titled *European i2010 initiative on e-Inclusion*, information and communication technology (or ICT) plays a key role in this area, too.

² European Commission, *i2010: A European Information Society for growth and employment*, June 2005
<http://europa.eu.int/information_society/eeurope/i2010/index_en.htm>.

The strategy, more to the point, is to make for better health care in Europe by bringing information technology to its member states' national and local health and social services. It is a strategy that had been outlined in the 2004 e-Health Action Plan—titled *e-Health: Making healthcare better for European citizens; an action plan for a European e-Health Area*—which sets out a joint planning initiative with measures for member states to adopt by 2009. There are three objectives that the 2004 e-Health Action Plan states: to develop shared strategies and methods common to all member states; to undertake joint actions aimed at speeding up the process of setting up e-health systems; and to work out best practices on the basis of these experiences and assess how e-health so managed can improve the lives of citizens.

For evidence that the EU is committed to the development of e-health, consider that the European Space Agency is funding research aimed at supporting e-health by way of satellite communications and at furthering the patient-centred approach to health care. The goal is to pave the way for a European e-health programme with the support of satellite technology, a programme to be developed in close collaboration with the World Health Organization.

Italy has itself recently launched projects based on the use of information technologies to deliver health services. Still, the only developments so far have consisted in the use of these technologies to manage and administer healthcare providers and institutions and help the people who run them. And then each of these providers and institutions has set up its own information system independently of the others, without a shared platform.

This will have to change in the future: information systems will have to be able to interact, thus making it possible to place greater emphasis on the patient's needs. Systems will therefore have to be so designed as to make it possible to share and access clinical and administrative information not only across a single healthcare facility but also between different such facilities.

A few systems have already been set up that connect different agencies and provide services covering entire communities, even regional ones, an example being the Centro Unico di Prenotazione, for scheduling appointments. Other services are international and consist of networks for sharing information and knowledge about diseases and clinical treatments.

Clearly, these objectives make it necessary for healthcare institutions to work together in the effort to develop interoperable information and

telecommunication systems, this with regional governments and the national government providing infrastructural support.

2. The Role of Law in E-Health

One way to appreciate the role of law in e-health is to consider the increasing reliance of health care on information and communication technologies (ICTs). And so much has this process developed—with these technologies becoming more and more an integral part of healthcare delivery—that we now have to revisit the whole idea of e-health.

It used to be that e-health consisted for the most part in making a massive use of the Internet as a tool by which to convey information to patients understood as “cases” to be treated or as passive “users” gaining access to the system. But we have since been progressively moving toward a different conception, with a use of ICTs that makes patients an

integral part of the system views them more as persons than as sick people.

The change under way is so deep as to warrant a new name for all the healthcare services that ICTs make possible: these are no longer called e-health but health informatics.³ This science does more than provide the technology for the health services themselves; it also covers back-office and administrative processes, enabling health providers, pharmacies, government agencies, and patients to efficiently manage the information they need to share, in such a way as to establish solid networks for healthcare delivery. Patients thus play a central role as active members of these networks and are clearly identified as such members.

We can appreciate, then, how important it becomes to manage patient data—especially the patient’s medical data—in a secure and legitimate way: the data stored and managed by an information system must be

³ V. L. Sauter, “Health Informatics,” University of Missouri, 2005, <http://www.umsl.edu/~sauter/health_informatics/whatis.html>.

processed in such a way as to protect the patient's privacy, with adequate security measures and under a scheme in which it is clear who bears responsibility for such data and what civil and criminal liabilities arise out of a failure to fulfil these responsibilities. So there are many legal issues that come up in connection with e-health, and they require the expertise of someone who is versed in the law but who also has a good grasp of all the technology (including wireless technology and the Internet) involved in the exchange of healthcare data, such as is managed by the health informatics systems used by different welfare programs.

3. Electronic Processing of Medical Data

Until a few decades ago, there was no heightened social concern about the handling of medical data, nor was there any special issue of privacy or confidentiality, since most of the data was exchanged between a patient and a family doctor, and since this was mostly done on paper or even orally. But that situation changed as the use of information technology to do medical research and provide health care (including prevention, diagnosis, and treatment) made it imperative to work out legislation under which to protect people from such processing of their data. Indeed, ICTs have transformed medical information into medical data stored and managed in digital format at every stage in the life of a medical file, from its creation, to its use in diagnosis and treatment, and to its maintenance for record-keeping.

So, on the one hand, medical data is apt to be used with a discriminatory intent in a way that can do serious damage to the person if no guarantees as provided; but on the other hand, using and processing the same data electronically proves indispensable for maintaining the patient's health, and indeed public health at large. In fact, there are great benefits to be gained by relying on information technology to manage medical data, since an electronic database can hold huge quantities of data that can be accessed and exchanged across wide networks in a matter of seconds. But with these great benefits also come great risks: precisely because the data is now accessible to a wide number of persons, both private and public, and precisely because it can be so easily accessed, compared, and reprocessed, the potential for its misuse has accordingly grown exponentially, and the persons identified by such data therefore stand a much greater risk of having their basic liberties and dignity curtailed through a breach of privacy or confidentiality.

The issue came to the attention of lawmakers in the EU, which in 1995 enacted Directive 95/46/EC. In Italy, this directive was initially

implemented by way of Law No. 675 of 1996: the guiding idea was to balance the need to process medical data against the need to protect the data subject's privacy, but both the processing and the protection were made a subject of *administrative* law, for it was the administrative agencies that were responsible for framing the rules and enforcing them. That framework changed in 2003, when the **Italian Privacy Code** went into effect,⁴ making the processing of personal data (including medical data) a matter of statutory law and stating (in a title entirely devoted to medical data) that while health professionals processing medical data for the purpose of providing health care are subject to an obligation of professional secrecy, the protection of the patient's privacy is no longer based on the traditional principle of the physician-patient privilege.

The Italian Privacy Code defines as *sensitive data* any personal data revealing (a) racial or ethnic origin; (b) religious or philosophical beliefs or political opinions; (c) membership in political parties, trade unions, or

⁴ Legislative Decree No. 196 of 2003, *Gazzetta Ufficiale*, Issue No. 174 of 29 July 2003, Supplemento Ordinario No. 123.

associations or organizations committed to any religion or philosophy or engaging in any political or trade-union activity; or (c) a person's health or sex life.

Medical data is singled out for special treatment as a subclass of sensitive data: the Italian Privacy Code thus establishes that medical data can be processed only for the purpose of providing health care, and only by authorized personnel, meaning health professionals and public healthcare providers.

There is a broad range of data that classifies as medical under the Code:⁵ the concept is understood to include not just data revealing a condition or disease affecting a patient, but any data relative to someone's state of health.⁶

⁵ J. Monducci, *Diritti della persona e trattamento dei dati particolari* (Giuffr , 2003).

⁶ J. Monducci and G. Sartor, *Codice in materia di dati personali: Commentario sistematico al D.Lgs. 30 giugno 2003, n. 196* (CEDAM, 2004).

Section 76 of the Code regulates data revealing a person's state of health and specifies that such data may be processed only for the purpose of protecting the data subject's health or that of other persons or the collectivity at large.

The health professionals authorized to process medical data may do so only on two conditions, namely: that the persons whose data they are processing are patients under their care, and that they are qualified to exercise their profession, meaning they are in possession of a formal degree or license.

The public healthcare providers authorized to process medical data consist of all the government institutions listed in Law No. 833 of 23 December 1978, as further amended. They include health authorities (known as AUSLs), hospitals, research institutes, pharmacies, and emergency departments.

Any processing of medical data done for any purpose other than that of providing health care falls outside the scope of the Code (as in the case of processing carried out for research), and the same goes for any processing carried out by anyone other than a health professional or healthcare provider.

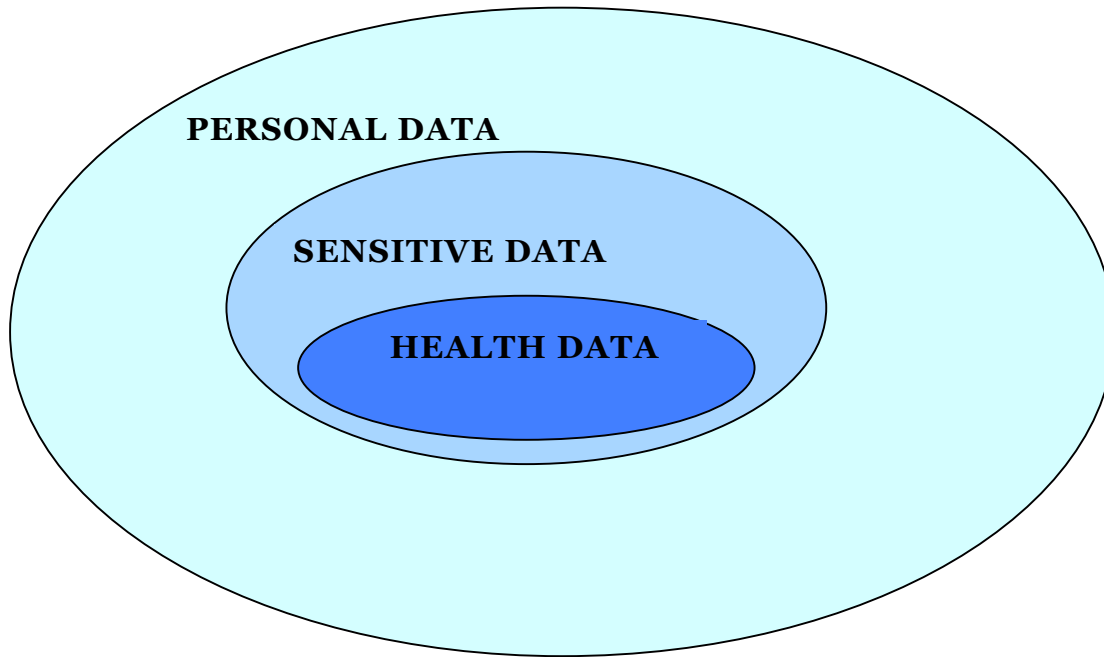


FIG. 1: Relationship among personal data, sensitive data, and medical data

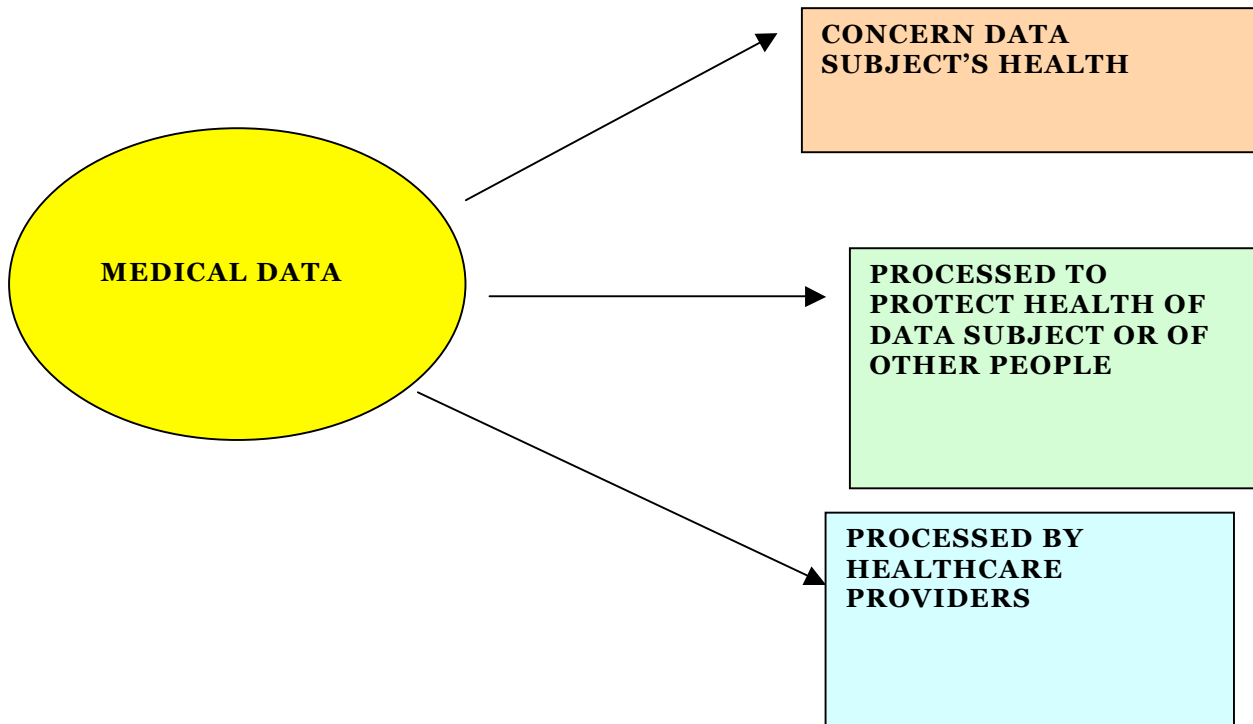


FIG. 2: Three requisites for medical data

One provision of the Code that is particularly relevant to e-health is Section 22(6), stating that if any sensitive data (and so also any medical data) is stored in digital databases, it must be processed by encryption techniques and identification codes, or by any method that will make the data unintelligible even to those authorized to access it, so that the persons the data refers to (the data subjects) cannot be identified except as necessary. And the subsequent Section 22(7) specifies that data revealing a person's state of health or sex life must be stored separately from personal data processed for purposes irrelevant to a data subject's state of health or sex life.

These provisions require minimum security measures, failing to implement which makes one criminally liable under Italian law. Thus Section 34 of the Code, on the electronic processing of data, states that data revealing a person's state of health or sex life may be electronically processed only on the condition of using encryption techniques or identification codes (among other minimum security measures).

Sections 22 and 34 combined thus require that any database containing medical data must be maintained using encryption techniques or identification codes and must be so designed as to separate the medical data from any data identifying the patient (as by name and surname or by a personal identification number).

Under Section 22(6) of the Code, the separation of data just referred to must be such that a patient will remain unidentifiable even to health professionals who are authorized to access the patient's medical data and have authenticated themselves for that purpose. Indeed, it is only at a later stage that such medical data can identify anyone, when the data that has been accessed is decrypted or an ID code is entered into the system. This rule is reiterated in Annex B of the Code, which sets out the minimum security measures that any organization processing personal data must implement into its own Internal Security Guidelines: these guidelines must state the criteria by which personal data revealing someone's state of health or sex life are to be encrypted and separated from all the other data identifying the same person. Thus any database containing personal data must keep the demographic data identifying a person physically separate from any data revealing that person's state of health.

Only by securely entering a unique patient ID code can the two sets of data be paired up. But otherwise, before such a code is entered, any data identifying a patient must be protected in the database by encryption: this will ensure that data revealing someone's state of health remains anonymous to anyone accessing the database without authorization. When data identifying a patient is so encrypted, it is displayed as garbled data unintelligible even to the health professionals authorized to access it. It therefore does not identify anyone except when necessary (as required by Section 22(6) of the Code), and it renders anonymous any matching data revealing the patient's state of health: only when the patient's ID code is entered by an authorized user does the encrypted information become intelligible (by decryption), thus making the matching medical data no longer anonymous.

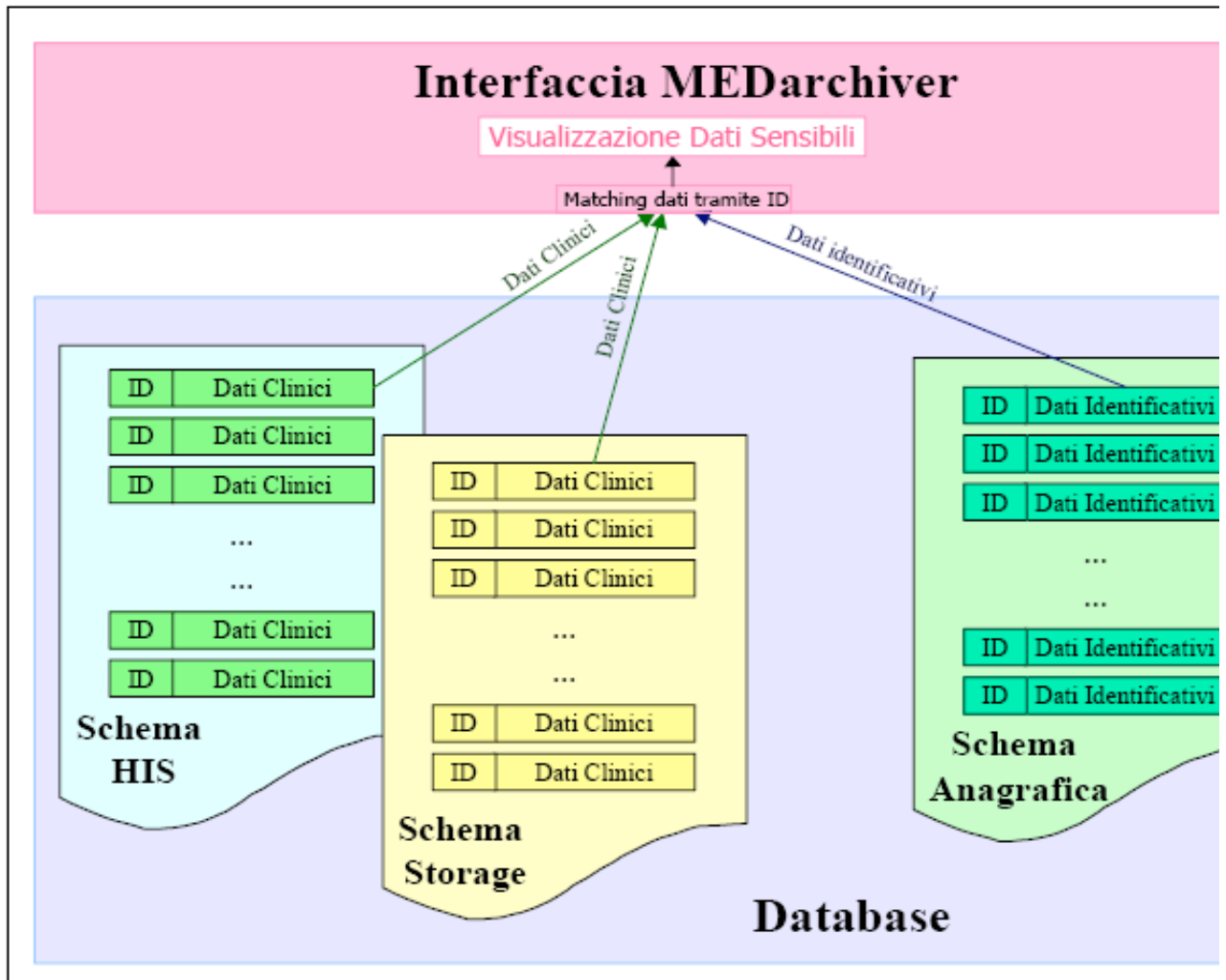


FIG. 3: An example of how medical data need to be organized in a digital database (courtesy of Medarchivier S.R.L.)

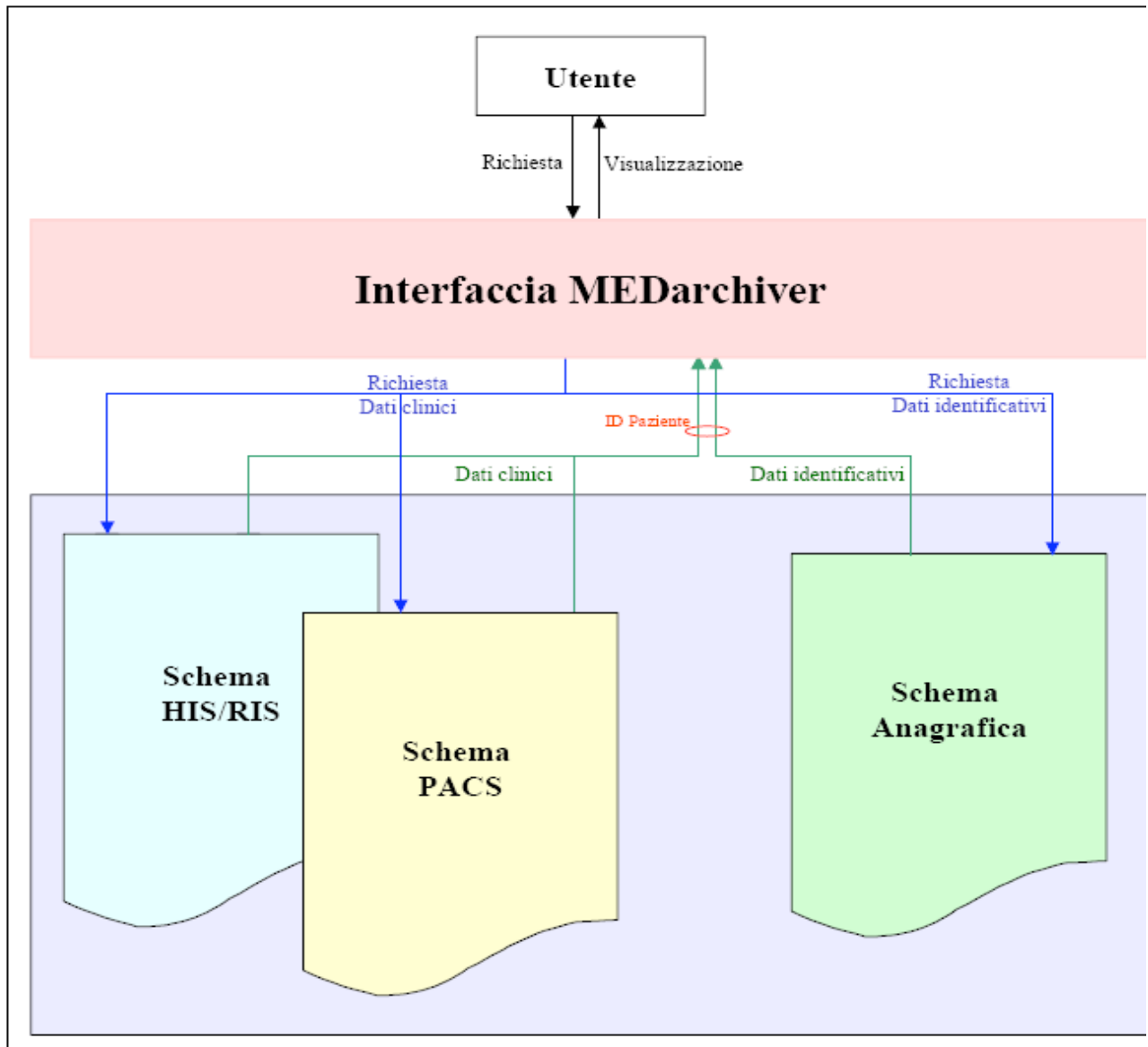


FIG. 4: The Medarchivier system for displaying medical data (courtesy of Medarchivier S.R.L.)

4. Electronic Health Records and the Law Pertaining to Them

No e-health system would be complete without a medical record in digital format. These electronic health records are a special case of electronic

records, which the EU recognizes as having legal validity and evidentiary force. The same status was first recognized in Italy with Law No. 59 of 1997, whose Article 15 provides that any record, document, contract, or other instrument drawn up, filed, or sent by a government agency or a private entity in digital format will be valid and enforceable under the law. This provision was then integrated into the Consolidated Guidelines on Administrative Record Keeping,⁷ stating that electronic records (defined as any legally relevant information represented in digital format) will be deemed legally valid regardless of who prepares them or how they are stored or delivered. The same provision has also been integrated into the Digital Administration Code.⁸ EU and Italian law thus

⁷ President of the Republic, Decree No. 445 of 28 December 2000: *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*, S.O., published in G.U., Issue No. 42 of 20 February 2001.

⁸ Legislative Decree No. 82, 7 March 2005, published in G.U., Issue No. 112 of 16 May 2005, S.O. No. 93, *Codice dell'Amministrazione Digitale*, amended by Legislative Decree No. 159 of 4 April 2006, published in G.U., Issue No. 99 of

both permit the use of electronic documents and records for any governmental or public function.

Much of the debate in Italy and abroad with regard to electronic health records (or EHRs) has focused on the issue of the information that should go into them and the technical characteristics they should exhibit. An EHR is a comprehensive record providing a wealth of clinical information about the patient: in addition to specifying the condition for which a patient was taken into hospital and later discharged, an EHR will also contain the patient's medical history, including an anamnesis (the patient's own or that of family members), as well as it may specify plans for future care (therapies) or even report information about his or her mental health.

Thus, in order for an EHR to serve any useful purpose in an e-health system, it will have to collect several *different* medical records and

documents from local sources and repositories distributed over a given territory. And that makes it necessary for an EHR to be thoroughly indexed and sourced, with metadata tagged to all the information in the EHR itself, thus indicating where all such information comes from.

It follows from this description of EHRs—as records collecting information from different sources—that the information they gather must be sharable: EHRs must accordingly meet the further requisite of interoperability. Which in turn means that they must share not only a structure but also a semantics for the information filling that structure, thus making it possible to extract such information in a uniform way.⁹ For this reason, shared standards are being sought under an initiative called Integrating the Healthcare Enterprise (or IHE), and one of the

⁹ This is achieved by way of a profile called Cross-Enterprise Document Sharing (XDS), enabling different healthcare organizations to share cross-sections of a clinical record and thus build a longitudinal cross-enterprise record that keeps track of a patient over time.

concerns in this effort is to settle on uniform methods for collecting the informed consent necessary to ensure a patient's right to privacy.

We can see, then, at this early stage, that while EU and Italian law both permit, and even encourage, the interchange of electronic health records and documents on the basis of uniform standards, there is also a parallel focus on the legal issues raised by this nascent practice.

In Italy, these issues arise in connection with the legal status of medical records as publicly authenticated documents (so-called *atti pubblici*). This view has consistently been upheld by the Italian Court of Cassation, which finds that medical records can serve as documentary evidence: they do so insofar as they are deemed to certify a patient's condition and because they share in the public nature of healthcare provision.¹⁰ So a medical record is not just *any* record (an administrative document like many others): the kind of information it contains and its use in certifying

¹⁰ See, among other judgments, Cassazione Penale, Sezioni Unite, No. 7958 of 11 July 1992.

a patient's condition place it high up in the hierarchy along which the Italian legal system arranges different types of documents. The Court of Cassation has also found that a number of medical documents in addition to the medical record are likewise deemed authenticated evidentiary documents: these include any of the medical documents making up a medical record (Cassazione Penale 10609/82), medical certificates issued by AUSL health authorities (Cassazione Penale 2207/1995), the medical charts maintained at nursing homes (Cassazione Penale 7958/1992), death certificates (Cassazione Penale 9073/1989), clean bills of health (Cassazione Penale 9191/1982), and the documents produced by a medical panel entrusted with certifying a person's disability (Cassazione Penale 1004/2000).

It should also be mentioned in this regard that an official making false representations in a document he or she draws up is liable to criminal prosecution under Articles 476, 478, and 479 of the Italian Criminal Code.

Thus any EHR system, and so any practice management software, will have to be designed taking into account the legal status of EHRs as evidentiary documents, along with the liabilities—both civil and criminal—of those responsible for drawing them up as well as for maintaining and storing them. The civil liabilities involved are attached in part to the obligations the Privacy Code sets forth in Section 92(1) with respect to medical records at large, requiring all healthcare providers, whether public or private, to ensure that the information entered in such records is clear and that the data pertaining to a patient is kept separate from other people having a legitimate interest in the patient's care. The point of this latter requirement is clearly to protect the everyone's right to privacy by making it so that when an EHR system is queried, the information retrieved is specific to the request and not bundled with any other information.

This is consistent with the finding of the Italian Data Protection Authority that any public healthcare provider authorizing access to a patient's medical record will first have to select the specific data the requester may access.

In summary, EHRs designed on the basis of international standards making it possible to easily share patient information when necessary is a welcome development in the healthcare sector. But at the same time, the design of EHR systems should also take into account all the rules of law, national as well as international, that apply to EHRs in virtue of their nature as evidentiary documents containing sensitive information instrumental to the function of healthcare delivery. Otherwise, EHR systems might not come into any standard use at all, meeting as they

would the resistance of wary patients and cautious healthcare providers concerned to protect themselves from the liabilities (administrative, civil, and criminal) that attach to a misuse of EHRs. Now, these liabilities have been put in place to make EHR systems *safer*, not riskier, to use, so it would be a paradox if such systems failed to take hold because perceived as putting all those involved in jeopardy.

5. Risk Management and Liabilities in E-Health

The advances made in medicine and the new technologies have been making us increasingly effective at preventing, diagnosing, and treating diseases: e-health, with its Internet and wireless technology, has improved access to the healthcare system and made it possible, among other things, to monitor patients more closely and provide for quicker, possibly lifesaving intervention. So there are at least two ways in which e-health can make health care more effective: it can cut down on response time (by making for better coordination among healthcare providers and patients) and it can improve prevention, by way of a close monitoring of patients that makes it possible to intervene early on.

Now, these expanded possibilities are introducing a tension into the system, for they are giving rise to legitimate claims to improved health care that current healthcare and welfare policy cannot yet fulfill. Indeed, while e-health can make the healthcare system more efficient and less costly in the *long* run, it requires in the *short* run infrastructural investments that cannot, or will not yet, be sustained.

E-health is thus bringing into the foreground the issue of two primary goods under constitutional protection: life and health. It is doing so by shifting the balance of discussion, just as it is shifting this balance with respect to the issue of healthcare data, making it necessary to work together two legitimate interests in potential contrast: the physician's interest in being fully informed about a patient's health and the patient's interest in keeping the same information confidential.

The physician-patient relation thus raises a privacy issue, as previously discussed, but it also raises another, no less important issue, which is that of the patient's informed consent: just as the physician has an interest in being fully informed about a patient's condition, so does the patient have a right to be fully informed about the nature of the treatment and the risks it entails. This principle rests on a strong foundation, to be sure, for it finds its legal basis in Article 13 of the Italian Constitution, which states that personal liberty is inviolable, and

which has been interpreted to include the human right to health and physical integrity. But while there is no question about a patient's right to be fully informed before consenting to a treatment, or about a physician's obligation to obtain such consent, the whole transaction may become meaningless when carried out through the technologies that e-health is built on.

Another, and equally important, legal issue that e-health is having us rethink is that of risk management in health care: this is the issue of the liabilities that medical as well as nonmedical staff may incur when risks have not been properly assessed and something goes wrong. To this day, the governing law in Italy remains Article 2236 of the Civil Code, stating that so long as health professionals do not act with gross negligence, they will not be liable (need not pay damages) for any healthcare adversity or failure owed to a treatment presenting an exceptional degree of difficulty. Now, clearly, this whole provision turns on what it is that makes a problem "exceptionally difficult" to solve, and this is a determination that can only be made on a case-by-case basis, for it depends on the types of instruments the health professional could have relied on.

This holds true especially for e-health, which relies on a range of instruments that open this clause to an even wider range of interpretations, regardless of whether the instrument in question is hardware (as in the case of robots) or software, in which case we have artificial intelligence systems used in diagnosis (with the support of imaging and other techniques) as well as in therapy (as when administering drugs). A branch of artificial intelligence relevant to e-health is that of expert systems: these too can be used to improve diagnosis, and they can also avert therapeutic errors that medical personnel are liable to commit in critical situations. There is, finally, the use of automated notification systems based on threshold values, and this is yet another technology with respect to which liability issues come up.

The technology used in e-health is thus forcing us to rethink our way of handling liability in the event of errors, especially so when such errors are owed to a malfunctioning software system: here, it becomes the jurist's task to decide how to apportion responsibility between the health professionals using the system and the system's creators, who might be the hardware manufacturers or the software developers.

An issue of accountability arises as well in connection with the knowledge base made available to physicians by online databases, information-retrieval systems, and other such ICT tools. This is to say that the vast amount of knowledge available, and the ease with which it can be accessed, makes it all the more impelling for physicians to make

sure they have that knowledge and that they use it daily in their profession. Which tends to raise the standard that physicians may be held to under the law for any treatment that should fail.

There is, too, the civil liability of the Internet service providers, network administrators, and other such technicians responsible for supporting an online e-health service.

The use of technology in healthcare provision gives rise to civil as well as criminal liabilities, each governed by its own standards: civil liability emerges in connection with the *security* that end users can reasonably expect from the technology they use; criminal liability is quite more stringent, for it is moving closer and closer toward a criterion of *prevention*, making it criminal to even put patients in jeopardy by exposing them to the *risk* of something bad happening.

And e-health, precisely because it is so dependent on the proper functioning of the technologies it employs, tends to amplify the hazards associated with healthcare delivery—it therefore calls for a scheme of liabilities that will take this risk factor into account. Indeed, there is not just a security risk at issue, namely, the risk involved in the transmission of medical data, but also a health risk proper, since any delay in the transmission of such data may have grave consequences for the patient's health, just as may happen if a robot or other technological system should malfunction. It follows that those responsible for these technologies—that is, the health provider managing an IT system or the manufacturer of a robot or other equipment used in healthcare delivery—may be held to a higher standard of liability (in the form of higher money damages) commensurate with the greater risk that the patients and healthcare consumers are exposed to.

Product liability thus intersects with medical malpractice liability. From a broader perspective, though, this liability issue makes it necessary to look at the interactions and agreements that take place between healthcare facilities, healthcare providers, and the manufacturers of medical equipment: jurists and health officials must understand how these parties interact with one another and who is responsible for what, for that will make it possible to allocate liabilities accordingly by contract. The same goes for the interactions that health providers have with online service providers and with the hardware manufacturers and software developers of the IT systems used in e-health: here, too, the problem will be to draw up model contracts on which basis to set out the guarantees that each party must make and the liabilities that may be incurred for failing to live up to those commitments—all the more so that the primary concern is to protect healthcare consumers, and that such fundamental values as life and health are at stake.

6. The Use of RFID Technologies in E-Health: Legal Issues

RFID (short for Radio Frequency Identification) deserves attention here for the same reason that all the other new technologies so far discussed do, which is that the advantages it brings also carry risks for the individual as well as for society as a whole. Specifically, its use may infringe certain basic rights, first among these the right to privacy. A debate is therefore under way, not only in Italy but also abroad, and especially in the United States, about regulating RFID technologies in such a way that these rights are protected.

Thus, by way of example, RFID is used in so-called smart labels: attached to the backs of regular barcode labels, smart labels make it possible to track goods as they travel. Which is useful, but at the same time it also makes it possible to track the *consumers* who use these products. More alarming still is that smart labels, as well as their housing and readers, are very small, which means that any personal data captured in the label can be retrieved and processed unbeknownst to the data subject.

There is in fact a whole menu of data that RFID can retrieve and collect relative to a data subject: any tagged item purchased by this person (including pharmaceuticals and services) relays information that, once collected, can be used to profile his or her consumer and travel habits and preferences. Furthermore, since the trend is toward adopting shared RFID standards, it is becoming increasingly easy for unauthorized third parties to access the information and reprocess it (as by “rewriting”). Then, too, RFID technology is making it possible to read labels at greater and greater distances, and the technology itself is becoming cheaper, which means that it is bound to come into wider use over time. We thus have a developing scenario in which more and more people can be located over greater and greater distances, and this doubtless raises issues about personal freedom.

This calls for framework by which to regulate this technology and protect consumers, who are entitled to know whether a product they buy has an RFID tag attached to it and, if so, to have it removed at the time of purchase. So, too, the data so collected should not be available except with the consumer’s free and informed consent, and the processing itself should likewise be regulated.

RFID, geo-localization, and other such emerging technologies have been the focus of a recent working paper by the Data Protection Working Party set up under Article 29 of Directive 95/46/EC. Similarly, in Italy, an

agency called CNIPA (National Centre for Information Technology in Administrative Government) has recently launched a feasibility study to assess the pros and cons of using RFID systems for administrative agencies across the country: the task has been entrusted to a study group working in association with the RFID Observatory of the Politecnico in Milan and with the RFID Lab of the Università La Sapienza in Rome. The technology is not in wide use today in government, but the idea is to see if it can help improve a range of public functions and services including document management, firefighting, emergency medical services, and civil defense.¹¹

One concern in the debate has been to make sure that data subjects know right away and up front when and how any data pertaining to them is being processed, and to this end the Italian Data Protection Authority has required the use of pictograms or other images alerting data subjects

¹¹ RFID is part of a broader range of technologies called Automatic Identification and Data Capture (AIDC), other examples being biometrics, smart cards, and bar codes.

whenever they are being filmed by a surveillance camera or are buying products carrying RFID tags.¹²

If consumers *generally* need to be protected against the use (and possible misuse) of RFID technologies, all the more should this protection be robust in health care. Indeed, the stakes here are much higher, for it is the integrity of the person and human dignity that may be put in jeopardy.

One medical use the technology has been put to is for human-implantable RFID microchips. This is a controversial use that for different data-protection commissioners across Europe fails to meet basic data-protection criteria. And even where these microchips have been approved,¹³ their use is regulated and there is concern about the

¹² Italian Data Protection Authority, general ruling on RFID smart labels, 9 March 2005.

¹³ One example is the United States, where such use was approved on October 12, 2004, by the Food and Drug Administration.

associated risks. In fact, the implant may pose a health risk in addition to the standard security risk, the latter of which becomes all the more alarming considering that the chips may carry medical data.

In 2005,¹⁴ the Italian Data Protection Authority ruled that human-implanted microchips do not meet data-protection standards: as a general rule, then, their use is prohibited because deemed in violation of human dignity (Section 2 of the Italian Privacy Code) and in violation, too, of human dignity and the right to the physical integrity of the person as these principles are set forth in the EU Charter of Fundamental Rights, Articles 1 and 3, as well as in domestic law. The same authority does, however, provide for an exception to the rule if compelling evidence is produced showing that the use of such microchips (a) is dictated by the need to care for someone's health, (b) is congruent with its purpose (Section 11 of the Privacy Code), and (c) does not in any way violate the data subject's dignity (Section 2(1) of the Privacy Code). A further condition is that the patient must be in a condition to have the

¹⁴ General ruling on RFID smart labels, March 2005, cit.

microchip removed free of charge and without interrupting the data processing for which the microchip was implanted. And the microchips themselves will have to be so designed that they can be implanted and used securely, in such a way that the information they carry, as well as their presence under the data subject's skin, remains confidential. If any sensitive data (and medical data in particular) is stored in a microchip, its processing must comply with the relevant requirements in the Privacy Code (Sections 2 and 22 and Part 2, Title 5) and is also subject to the Data Protection Commissioner's authorization pursuant to Sections 26 and 76 of the Code. Data controllers (health providers and medical personnel) requesting such an authorization may be required to submit to an assessment by the Data Protection Authority to make sure the use sought for the RFID tags in question does not infringe any of the data subject's rights or his or her dignity. Finally, any processing of medical data captured using RFID tags must comply with the security requirements discussed earlier in Section 3, the point being to make sure as far as possible that no data is lost or destroyed (not even accidentally) and that no unauthorized access occurs.

As with any processing of medical data, so here too—where the processing is based on RFID technologies—we have to think about what happens if an error is made or a malfunction occurs; that is, we have to ask what civil and criminal liabilities should arise out of injuries connected with these technologies and how these liabilities should be allocated between manufacturers and medical personnel.

If an RFID system should malfunction, or should fail to guarantee secure data transmission, or should delay such transmission, the injury for the patient could be serious indeed, and it could therefore make the system's developer or the health provider using it liable to steep penalties (money damages) designed to protect patients in the face of the greater hazards to which the technology exposes them, all the more so if these hazards are life-threatening, as happens when RFID technologies are used to treat patients with heart conditions or diabetes (in the latter example, the implanted microchip measures blood-sugar levels, and the patient doses the insulin accordingly). Here too, then, it can be appreciated how product liability intersects with medical malpractice liability, and the issue must therefore be considered from the broader perspective of the formal and informal agreements making up the whole web of relations connecting patients with physicians, healthcare facilities, service providers, manufacturers of medical devices, and the developers of the corresponding software.

7. Conclusion

In conclusion, it bears stressing the Janus-faced nature of technological innovation, which improves the quality of life and advances our knowledge, but at the same time it is apt to be misused in such a way as to violate basic human rights. Thus it would be a mistake to regard a new technology as *inherently* good: we have to think about the possible adverse effects of its use and misuse and must work out shared criteria designed to forestall such effects.

That holds all the more true when the technology in question involves human health (as does all e-health technology). A legal analysis of its use will have to go beyond a cut-and-dried implementation of all applicable rules and regulations: it will instead require that the systems and their components be fully understood, along with all the services offered through them. Accordingly, it does not suffice to point out the legal safeguards set up to ensure that an e-health system does not make patients vulnerable and does not violate any of their rights: a legal analysis should further assess how these safeguards work in practice and should offer solutions to make them effective if that is not the case. The trick is to make these solutions not only valid from a legal standpoint, but also technologically and economically sensible.