Position Paper: Transparency in Network Chains – Legal Dimensions

Sjaak Nouwt and Corien Prins

Tilburg University, Center for Law, Public Administration and Informatization,
P.O. Box 90153, 5000 LE Tilburg, The Netherlands
Phone: +31-13 466 8199, e-mail: J. Nouwt@uvt.nl, J.E.J.Prins@uvt.nl

Bernd van der Meulen and Marieke Lugt

Law and Governance Group, Wageningen University, Hollandseweg 1 6706 KN Wageningen, The Netherlands
Phone: +31-317 482957, e-mail: Bernd.vanderMeulen@wur.nl, Marieke.Lugt@wur.nl

1. INTRODUCTION

In this position paper we present a first insight into the legal dimension of transparency in network chains. Clearly, information is a key driver needed to successfully implement and realise transparency in network chains. Thus, transparency in network chains is highly dependent upon the extent to which information may be (freely) used, processed and transmitted within network chains. The actual extent to which information may be used and transmitted within network chains is determined among others by legal rules and regulations. In other words, the law interrelates in many ways with information and information processing and the outcome of this interrelationship influences the amount of transparency that may be realised. In addressing this issue many questions arise: Who owns information and data? Who is under what circumstances responsible for information and the distribution of information? Under what conditions may information be used? What security or even secrecy obligations apply? In a network environment various parties use and transmit information. The answer to the afore-mentioned questions may differ from party-to-party. Also, the answers may vary depending on the type of information at stake (personal information, commercial information, copyrighted information, etc.).

This position paper aims at providing an overview of the various dimensions of the interrelationship between law and network transparency, between law and network partners, between law and network information. It explores the legal implications as well as presents topics for further research when it comes to optimising transparency in network chains. The central question addressed is: what legislative and regulatory frameworks apply and what legal questions arise when processing and distributing information and data within network chains?

On the basis of two case studies (the medical network chain and the food chain) we identify critical legal issues that parties in network chains face in light of using, processing and transmitting information through network chains. We elaborate on the relevant rights and responsibilities that arise. Furthermore, we discuss legal implications and uncertainties of use of information within network chains, e.g. conflicts between intellectual property rights and privacy protection. Finally, we draw – based on the outcomes of the two case studies, general conclusions as regards the extent in which the law influences transparency within network chains and the role that actors in such chains may play in setting legal standards.

Before embarking on an analysis of the two case studies, we will first introduce the key legal issues that relate to information and the use of information.

2. INFORMATION: BALANCING EXCLUSIVENESS AND GENERAL ACCESS

As has been said many times before: information is nothing more than money and power. This is true for our present-day information society, but it was true also when it came to ownership and use of information several decades ago. The advent of Information and Communication Technology (ICT) has however, renewed and intensified the debate on balancing interests: the general interest in guaranteeing the freedom of information and the interests of individuals in protecting their exclusive rights to information (privacy and intellectual property).

ICT influences a variety of societal, economic and social processes and phenomena. Technology is becoming, as it were, interwoven with our society. It more or less goes without saying that the dilemmas directly connected to the key object of this new society – information – thus demand our immediate attention. The ICT dominated society is referred to as an information society with good reason: information, data and knowledge constitute the driving forces behind a great many processes. A central issue is then: who may and must have disposal over what information and for which purposes? Focal concepts in this respect are the exclusivity of certain information and the property rights to that information on the one hand and free access and general distribution of information on the other hand. Information is a factor that in the one case, as an individual, economic and intellectual value, demands legal protection but, in another case, free access and free dissemination of information is crucial in light of certain values and interests, among them transparency in network chains. The current dilemmas concerning power over information are evident in many areas. Various interests underlie arguments to keep information in the exclusive domain of certain parties.

A first example is intellectual property right. Monopolies in information exist on the basis of copyright and database rights and owners of such rights use their monopoly to determine the conditions under which information may be used, re-used and extracted from databases. Various collections of information gathered by private as well as public parties (statistical information, commercial information, marketing information, environmental data, real estate and land information, addresses for persons and companies, vehicle information, etc.) will qualify as databases and could hence be protected under database law. Other works may come within the ambit of copyright law. The question arises as to what extent the owner of such information may restrict others to use this information within network chains.

A second example relates to privacy. In many countries, the right of privacy is expressly recognised. Some countries have included it as a fundamental right in their constitution, whereas others protect privacy interests at a lower legislative level or have recognised it in case law. In addition, international treaties and other international rules (such as the European Directive 95/46/EC on personal data protection) expressly refer to the status and maintenance of this fundamental right. Obviously privacy, and more specific data protection, has an effect on the scope in which use can be made of (electronic) information that qualifies as personal data.

Thirdly, mention must be made of liability concerns and the effect of such concerns on the extent to which information may become available. In providing access to information and distributing such information within network chains, a party in this chain may cause damage to other parties. It might, for instance, distribute information without a proper copyright licence, it may make incorrect or incomplete information available while somebody relies on it, it may make information available that breaches somebody's informational privacy. If a party performs these or other unlawful acts, it might very well be held liable for the damage that the victim suffers. Whether this party is really liable will generally depend on whether its conduct was reprehensible. The party will be considered liable if it was reckless or careless in distributing the information, for example in case it knows that its employees are making incorrect (e.g. outdated) information available to others within the network chain and took no action to correct the situation. Another example: through a security problem in the information system of a party, personal data about somebody became available to other parties in the network chain (constituting a breach of this person's informational privacy).
On the other hand, a party may face liability if it fails to fulfil a legal obligation to provide certain information within the network chain.

Fourth, competition law is suspicious of agreements between market parties to exchange information. The main reason for competition authorities to be concerned with information exchange agreements lies in the potential of these agreements to facilitate collusive behaviour among competing undertakings (as companies are usually called in competition law), since they are likely to improve the monitoring of activities of competitors.
In competition law a distinction is made between public and private market transparency. Public market transparency is transparency for consumers, while private market transparency is transparency for undertakings. It has been argued that public market transparency is essential for competition, since it allows consumers to effectively compare products and services. This kind of exchange of information will therefore intensify competition. Therefore, the publication of prices, for example, via advertisements will increase both public and private market transparency. On the other hand, private market transparency only increases transparency for the undertakings involved and may, through collusive behaviour on prices and output, have an adverse effect on competition. Indeed, in terms of effect on competition, public market transparency can be seen as the opposite of private market transparency. As a consequence thereof, private market transparency will be the main concern of competition authorities.[1]
The Netherlands Competition Authority (NMa) for instance took enforcement measures against the Royal Dutch Hairdressers' Federation (ANKO) a branch association to which approximately 6200 hairdressing salons are affiliated. In November 2000, in a letter to its

[1] Faull & Nikpay, The EC Law of Competition, Oxford University Press 1999.

members, the association indicated that its members should reassess their price lists because prices would increase on average by 5 percent in the year 2001. NMa ruled that by providing this information ANKO acted in conflict with the prohibition on cartels.[2]

The above four examples show that various legal interests may restrict the free flow of information within network chains. There are, however, also obvious reasons and interests for enhancing availability of and access to information in certain network chains. One of them being that the demand for information is the binding factor in a variety of interests related to such networks. For certain actors in network and information chains the possession of information usually translates into power. The collection, storage and processing of information and the opportunities to generate highly personalised decisions based upon this information, are becoming central steering instruments for both the private sector as well as the public sector. Access to information is crucial to guarantee a fair and transparent government. Access to information allows insurance companies to better calculate certain risks in advance. In other words, the social, democratic and commercial value of information is a key factor in determining the role and position of the various actors in network chains.

A single conclusive answer cannot be given when balancing the interest of exclusivity of information on the one hand and the interest of general access and availability of such information on the other hand. In order to get a more focused insight on the relevant interests as well as the rights and obligations that apply when balancing the interests we analyse two specific domains: the food chain (section 3) and the health care chain (section 4). In discussing both chains we will also determine the responsibilities as regards the use of information within network chains (e.g. responsibilities related to the security of the information and information processing). The principle reason for choosing these two domains is that they differ in the type of information (product information versus personal data) and thus the rules and regulations that have an impact on transparency within these chains. Also, the underlying reasons for establishing transparency within the chains and thus the traceability obligations that apply differ in both domains.

3. THE FOOD CHAIN

3.1 General introduction

In the food sector in Europe a regulatory reform is in full process. From the beginning of the European Community in 1958 until the mid-nineties the major aim of European Food Law was to facilitate an internal market for foodstuffs. This economy oriented legal framework proved incapable of coping with food safety scares like the BSE and dioxin crisis. In response to these shortcomings both the Food industry and the European Commission took initiatives aimed at providing legal instruments to deal with food safety problems.

A common feature in these initiatives is a move towards production chain integration. After all quality flaws at any stage in the food production chain can have their effects all down the production chain. Three infamous food scares – the BSE, dioxine and MPA crisis – had their origin in the feed of food producing animals.

Using contract law instruments industry – often at the initiative of the retail sector – creates certification and quality guaranty systems.

The European Commission published in the beginning of the year 2000 a White paper on Food Safety. This White paper indicates 84 measures in the field of policy and legislation aimed at restructuring the body of food law in such a manner that the focus in the first place is on food safety.

A major legislative step in the creation of the new regulatory framework was taken in 2002 when the so-called General Food Law[3] (hereafter: 'GFL') entered onto force. Further pieces of legislation follow suit.[4]

3.2 Regulations on transparency

3.2.1 Self-regulation

In case industry creates its own legal framework on the basis of contract law instruments, we often speak of self-regulation. Self-regulation can be an alternative for legislation, but it can also be an answer to the demands of new legislation and sometimes the law even creates obligations to self-regulate.[5] In the latter situation one might speak of 'enforced self-regulation'.

In the field of food safety self-regulation to a large extent seems to be an autonomous response to food safety problems and the reactions they provoke from consumers. Contract law chain integration occurs on the national[6] level as well as on the international level.[7]

The achieved quality standard can be communicated to the consumer by means of quality certificates. Within the network, enforcement mechanisms are in place. Participants agree to submit to audits. If the results of these audits are not satisfactory, participants may be excluded from the use of certificates and other rights. The information flow within the chain consists mainly of product-information. Therefore privacy legislation does

[2] Case 2234/ANKO www.nmanet.nl

[3] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.

[4] E.g. on gmo's and food and feed controls.

[5] Food hygiene law for instances provides for the introduction of HACCP-systems which are devised by the concerned enterprises but which are enforced under public law. See: Proposal for a Regulation of the European Parliament and of the council on the hygiene of foodstuffs, COM(2000)438 final – 2000/0178(COD).

[6] In the Netherlands amongst others: Stichting Keten Kwaliteit Melk (Foundation for Quality in the Milk Production Chain).

[7] EurepGap, Global Food Safety Initiative. See www.ciesnet.com.

not raise the same questions, as we will encounter hereafter in the health chain.
Complications may arise from competition law. Self-regulation of food safety is likely to fall within the scope of the ban on cartels. In the Netherlands however most applications for exemptions are granted by the NMa, except when so called hard core restriction are made like agreement of prices and market shares.

3.2.2 Legislation
In the food sector a regulatory framework is being built that requires – and therewith in a legal sense enables – producers to hand down information through all the stages of the product chain. Labelling prescriptions ensure that the ultimate consumer is provided with information concerning the composition of the product and to a certain extent concerning the way it has been produced (organically? genetically modified?) or treated (pasteurised? sterilised? irradiated?) its geographical origin and production unit (batchcode). This paper in particular focuses on the transfer of information between stages in the chain.

In Europe Food Law is in a stage of transition. The role of the European Union is increasing and the role of the member states is decreasing.[8] At first Community legislation on foodstuffs concentrated on questions of trade and free movement of goods. Today new goals have been added: a high level of protection of public health, safety and of consumer protection. A wholly new structured body of legislation is in preparation. As mentioned above: an important step is the introduction of the so-called General Food Law. The GFL takes a comprehensive and integrated approach to food safety. It uses a broad definition of food law covering a wide range of provisions with a direct or indirect effect on the safety of food and feed, including provisions on materials and articles in contact with food, animal feed and other agricultural inputs at the level of primary production (art. 3-1).
According to the GFL's preamble, experience has shown that the functioning of the internal market in food or feed can be jeopardised where it is impossible to trace food and feed. It is therefore deemed necessary to establish a comprehensive system of traceability within food and feed businesses so that targeted and accurate withdrawals (the well-known recalls) can be undertaken or information given to consumers or control officials, thereby avoiding the potential for unnecessary wider disruption in the event of food safety problems.
Therefore it is deemed necessary to ensure that a food or feed business including an importer can identify at least the business from which the food, feed, animal or substance that may be incorporated into a food or feed has been supplied, to ensure that on demand traceability can be assured at all stages. Also downstream information must be available. To this end food and feed business operators shall have in place systems and procedures to identify the other businesses to which their products have been supplied. This information shall be made available to the competent authorities on demand (art. 18). Thus the GFL provides a legal basis for this specific form of transparency in the food chain.
The GFL provisions on traceability will come into force on January 1 2005. As a regulation the GFL will have direct effect upon market parties. Nevertheless the European Commission and the Member States intend to provide detailed provisions to facilitate its implementation. It seems unlikely, however, that the Commission and the Member States will reach agreement in time for these provisions on the details to be in place by January 1 2005. Therefore the burden to work out these details will be on industry.

At this moment traceability obligations are limited to specific sectors. In the meat sector for instance it must be possible to trace meat and meat products from the retail outlet back to the farm of origin. This sector was the first one in which traceability obligations were imposed amongst others in reaction to the BSE-crisis. We will come back to the meat sector in § 3.4 and § 3.5.
A second sector in the food chain where the system of traceability has just been introduced is the GMO sector. A Regulation on traceability and labelling of GMOs and traceability of food and feed produced from GMOs (Regulation (EC) No 1830/2003)[9] laying down comprehensive traceability requirements for GMOs as well as food and feed produced from GMOs entered into force on 7 November 2003. In addition to these legal requirements a system of "Identity Preservation" (IP) has been introduced by industry in reply to the consumers' wish to be provided with the opportunity to make informed choices on the purchase of foodstuffs with or without genetically modified organisms. A system of traceability has been set up by means of documentation and certification from the manufacturer of for instance soy in South America till the manufacturer of the final foodstuff in Europe.
Traceability is not only a top down legal prescription. Retailers have increasingly managed the food chain to ensure high standards that can be proven by audit using the instruments mentioned in § 3.2.1.

3.2.3 Enforced transparency
The GFL states that food law shall be based on risk analysis. In the GFL 'risk analysis' means a process consisting of three interconnected components: risk assessment, risk management and risk communication (art. 3-10). The third step is of particular relevance for this

[8] Before 2000 European provisions on food law usually took the form of directives (which have to be implemented in national law) after 2000 the European legislator is inclined to rather choose regulations (which have direct effect without any interference of Member States.

[9] Regulation (EC) No. 1830/2003 of the European Parliament and of the Council of 22 September 2003 concerning the traceability and labelling of genetically modified organisms and the traceability of food and feed products produced from genetically modified organisms and amending Directive 2001/18/EC, OJ L 268, 18/10/2003, p. 24.

paper. 'Risk communication' means the interactive exchange of information and opinions throughout the risk analysis process as regards hazards and risks, risk-related factors and risk perceptions, among risk assessors, risk managers, consumers, feed and food businesses, the academic community and other interested parties, including the explanation of risk assessment findings and the basis of risk management decisions (art. 3-13).
Risk communication demands a high standard of transparency not only within the production chain but also for public authorities and consumers. Public authorities may even provide the general public with information originating in or related to the production chain. Article 10 GFL explicitly states: 'Without prejudice to the applicable provisions of Community and national law on access to documents, where there are reasonable grounds to suspect that a food or feed may present a risk for human or animal health, then, depending on the nature, seriousness and extent of that risk, public authorities shall take appropriate steps to inform the general public of the nature of the risk to health, identifying to the fullest extent possible the food or feed, or type of food or feed, the risk that it may present, and the measures which are taken or about to be taken to prevent, reduce or eliminate that risk.'[10]
The system of contemporary Dutch food law is slightly different. In case a food product poses a health risk, the Consumer Goods Act (Warenwet) attributes to the Minister of Public Health the power to issue an administrative order to the food business operator concerned to warn the public. Only if this order is not heeded, can the Minister himself issue a public warning.
The difference seems subtle, but might be significant from a point of view of damage control. In most cases a food business operator is likely to prefer to handle the communication to the public himself. A warning issued by the authorities might cause considerable harm to the reputation of the product and the business associated with it, which can be the producer but also the retail outlet.[11]
These examples show that transparency can be forced upon the parties in the food production chain. They can be forced to disclose information and – on top of this – public authorities can disclose information concerning the parties to the network chain.
In the Netherlands the consumers' association (Consumentenbond) has shown itself dissatisfied with the existing possibilities for consumers to acquire information with regard to consumer products including food. At the end of 2002 they proposed the introduction of a bill on transparency of production and chains. Government has rejected this proposal. At this stage therefore consumers are lacking an instrument to impose transparency on their suppliers. They do however to a certain extent possess indirect instruments. In the Netherlands a Freedom of Information Act (Wet openbaarheid van bestuur) exists which gives them, within certain limits,[12] the possibility to claim access to information which rests with public authorities. In other words, if the public authorities acquire information from the production chain, this information may come available for consumers as well.

3.3 Traceability
The General Food Law uses a far-reaching definition of 'traceability'. It means 'the ability to trace and follow a food, feed, food-producing animal or substance intended to be, or expected to be incorporated into a food or feed, through all stages of production, processing and distribution' (art. 3). The GFL is very short however about the content of the requirement of traceability (see § 3.2.2).

3.3.1 Identity Preservation
Consumers' wishes to be provided with gmo-free food products have necessitated industry to come with their own systems. For the meat industry these systems should start of the very beginning of the feed chain. What this means can be illustrated by the chain of soy for feed. Annex 1 gives a graphic representation of the soy feed chain. Between every party (in the diagram represented by a box) along with the soy (products) information must be transferred. Within each box it must be assured that the soy – especially when it is being processed – and the information relating to it do not get disconnected.[13]
It should be borne in mind that the food production chain follows after the feed chain and is of – at the very least – a similar complexity.
At this moment five different arrangements are being used to ensure that soy feed is gmo-free.[14]

1) The supplier declares his products to be gmo-free.
2) Declaration of origin: the supplier declares his products to originate from a recognised gmo-free area.
3) Declaration and analysis. The supplier declares his products to be gmo-free and provides a certificate of analysis with each delivery.
4) Gmo-free supply chain certificate. This certificate represents procedures and registrations to ensure segregation throughout the production chain.
5) Identity preservation. IP is a management system of crops, raw materials and trade which aims to identify the origin of the product concerned.

[10] Risk communication is not as yet fully developed. Alerts from the rapid alert system are published weekly on the website of DG Sanco.
[11] Rumour has it that retail outlets are much more keen to recall products of other brands than of products carrying their own brand. A recall constitutes good advertisement for the company that takes the initiative, but it brings bad publicity to the product concerned.
[12] Secrets of trade and industry for instance are not available.
[13] The pending proposal for a Regulation on the hygiene of foodstuffs prescribes that food business operators (except those operating at retail level) shall ensure that foodstuffs produced by them are identified with an identification number.
[14] C.W.G. Wolf, M.W. Hoogeveen and J.J. de Vlieger, Ggo-vrije veevoedergrondstoffen voor de melkveehouderijg, Borging, beschikbaarheid en kosten, LEI 2003.

These five arrangements as numbered above provide an increasing amount of certainty but also increasing costs. Therefore it is likely that the best systems will only be chosen if they provide competitive advantages or if they are prescribed by law.

3.4 Relevant Parties

Food Law is chain based. It applies from 'farm to fork'. The information network that has to be in place covers both public authorities and companies in every stage of the food chain, including feed for animals that are intended for human consumption. European Food Law is relevant not only for parties within the EU, but also for companies and authorities in third countries that wish to export to the EU.

Inspectors from the Food and Veterinary Office (FVO)[15] carry out inspections in member states of the European Union and in third countries. Non-compliance with food safety or traceability regulations may have consequences on the export to or within the EU.

To give an example: the meat chain consists roughly of: farms, slaughterhouses, cutting premises, meat processing establishments, cold stores, distribution centres, retail outlets and the transports in between.

3.5 Legal Issues

The part of the meat sector concerning cattle and beef is interesting because a legal framework is in place that enables interested parties to transfer information throughout the whole production and trade chain.

This specific sector provides a glimpse of the future situation in the entire food and feed sector. Under the Generasl Food Law it should be possible for actors in the food sector to achieve any level of transparency they desire. However, reality in the meat sector seems to be far removed from this picture. The framework is not functioning satisfactory. To some extent at least this seems to be a problem of enforcement.

The FVO carried out a mission in the Netherlands from 18 to 28 March 2002 in order to evaluate the operation of controls over the traceability of beef and beef products.[16] This mission led the FVO to the findings that several authorities are involved in controls over traceability of beef and minced beef, but that responsibilities were not always clearly attributed. The supervision and control of the tracing of beef and minced beef, and the use of correct labelling, were insufficient.

All holdings and bovine animals should be registered and given a unique registration/identification number. However, some serious irregularities were found concerning animal identification, which could jeopardise the reliability and the accuracy of the system.

According to the FVO the identification system does not provide the necessary information to allow the tracing of animal movements satisfactorily.

The FVO found that tracing within the food processing chain was in many cases only possible using the information on the meat labels. Paper documentation was in most cases incomplete and/or unreliable. In several cases wrong information regarding the origin of meat was printed on labels due to failures in the registration and traceability systems. In no case was it possible to get the full documentation to allow traceability back to the farm(s) of origin.

These findings in a context where transparency is obligatory especially raise legal questions concerning the powers and the lack thereof to enforce transparency-obligations, and liability for damages which might occur due to insufficient availability of mandatory information.

Can companies be held liable for inconsistencies that have taken place upstream in the food chain, maybe even outside the EU?

It seems likely that the answer is affirmative. Traceability helps to limit recalls to only those products that are actually affected. If no functioning traceability system is in place the quantity of suspected products will increase and there-with the losses for the producer concerned. If it turns out that due to a lack of traceability products had to be recalled that were of good quality, the party responsible for this defect may be held liable.

4. THE HEALTH CARE CHAIN

4.1 General introduction

In contrast to the food chain, there is no specific regulatory framework in place in the health care chain that requires – and therewith in a legal sense enables – the relevant parties to hand down information through all the stages of the health care chain. Also, no legal framework is in place that enables interested parties to transfer information throughout the whole chain. This does not mean that no incentives are available to stimulate the transfer and processing of medical data between various participants in the health care chain. Here, the development of chains and networks seems to be very much linked to the introduction of new technologies (ICT) and not so much as a result of legislative intervention. In 1996, the Dutch Council for Public Health and Health Care (Raad voor de Volksgezondheid en Zorg) strongly advised the minister of Health, Welfare, and Sport to introduce ICT in health care, to be able to guarantee the quality of health care information, and promote the adequacy of the information exchange.[17] The Council pointed at three different but cohesive

[15] FVO is a section of the Directorate General Health and Consumer Protection (Sanco) of the European Commission. It is stationed in Grange Ireland. All the FVO reports are published on DG Sanco's website. See the next foornote.

[16] FVO reports are published on the internet. For the report on the above mentioned inspection see: http://europa.eu.int/comm/food/fs/inspections/vi/reports/netherlands/vi_rep_neth_8536-2002_en.pdf

[17] *Informatietechnologie in de zorg.* Advice by the (provisional) Council for Public Health and Health Care to the minister of Health, Welfare and Sport. Zoetermeer, October 1996.

applications: the health care chipcard, the migration from paper patient records to electronic patient records, and the use of the electronic highway (the internet) in health care information transmission and enabling health care providers to access electronic patient records by using a health care chipcard. A brief glance at the present situation, shows that the Council's recommendations have not yet been fully realized. Enhancing the quality of information and the adequacy of information exchange are still important goals to be realized by means of ICT. The step towards the further implementation of chains in which various health care professionals participate could be an important facilitator in realizing these goals. However, information exchange within such chains will be limited under certain circumstances by legal rules and regulations. For, sharing (patient) data is faced with questions surrounding ownership of data, responsibility of their use as well as other rights and obligations of the different partners within the chain.

Whereas in the food chain, the information at stake was not primarily related to individual persons, the health care chain deals almost by definition with (sensitive) personal data. The term used for this type of data is 'patient data'. Under the relevant Personal Data Protection Act (Wet bescherming persoonsgegevens) 'personal data' means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[18] 'Patient data', as we use it in this section, means personal data concerning a person's health.[19] This is a broad definition, which relates to all data concerning the physical and psychological health of a person. The definition includes information about a physical handicap, and information about the fact that someone is ill, although it does not give any information about the kind of illness.

In line with the theme of this position paper, we will focus on the processing of patient data in the health care chain (see below). The health care chain is focused on 'cure' and 'care'. Within this chain, patient data are used in different contexts and by various health care providers. The context may for example be the hospital, or the general practioner's office. Health care providers who may use patient data or may have access to them, are for example a specialist in a hospital, whether or not a 'treating doctor', a general practitioner, or a home care nurse. Consequently, the participants in health care chains are confronted different categories of patient data. The first category related to the patient's communication data (such as Name, Adress, and Domicile (NAW)). The second category is financial and administrative data, which are required for administrative purposes of the institution or professional practice concerned. Examples of such data are: data relating to the treatment of patient followed and to be followed, medicines or facilities provided, data concerning the calculation, determination and collection of the fee. Finally, the third category are medical data, or personal data concerning to a person's health. Thus, in discussing the legal aspects of information processing within health care chains it must be kept in mind that different types of data must be considered in light of their legal status. Also, some data may be relevant under different categories (e.g. data on prescriptions will be relevant for both the second and third category).

4.2 Transparency

When considering transparency in network chains, it is important to note that the term 'transparency' may have different meanings in the context of health care chains. We can understand transparency in health care chains in at least two different ways, both of which will be discussed in this section.

The first type of transparency in health care chains relates to transparency from the perspective of the data subject, i.e. the patient. According, for example, to the Openness Principle from the OECD Privacy Guidelines (1980), "there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller." As will be discussed underneath, this transparency principle is incorporated in certain legal obligations of the earlier mentioned data protection law.

The second type of transparency relates to the perspective of the health care provider. Health data chains make it easier for health care providers to have access to patient data. In other words, the patient and his data become more transparent for health care providers. Having better access to patient data, can improve the quality of health care. Health care providers are better informed, they can base their decisions on more information, and the patient is not required to fill in multiple medical inquiries. As will be discussed, the availability of (more adequate) information has an impact on liability standards applied to the different parties within a chain.

4.3 Network environments in health care

In focusing on the present Dutch situation, we note that patients may relate to numerous providers of different health care services. Whereas in the near past, each of these providers stored the relevant data in their individual

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal* L 281 , 23/11/1995 p. 0031 – 0050 (article 2).

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal* L 281 , 23/11/1995 p. 0031 – 0050 (article 8). Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens), *Stb.* 2000, 302, article 16, and 21.

systems (such as a stand alone GP information system) and communicated by means of paper-based mechanisms, recent developments show a clear tendency that various providers link their data registrations and information systems.[20] This process of connecting all relevant information systems slowly leads to future concepts of e-health and Electronic Patient Records. E-health means that telemedicine, knowledge management, diagnoses knowledge systems, distance cure, ultimately optimized administrations, communication from and between patients, health care professionals, and health care organisations will improve the quality and efficiency of health care. Within an e-health environment, Electronic Patient Records (EPR) will play a central role. More often, electronic storage of, and access to patient records are needed for specific applications of information and communication technologies. Combined, the various applications become one entity, in which patient data incorporated in an EPR will be accessible for every health care application. Of course, this requires a system of publicly accessible and general IT-provisions. In addition, a standardized system of data formats, application interfaces, and technology choices is needed. Only when these elements of infrastructure and standardization are adequately addressed, an overall IT-architecture of health care can be realized in which chain interaction and chain management plays a key role.

Several examples of health care chains can be mentioned, e.g. the CVA health care chain.[21] This chain is also the subject of a project of the Dutch organization CBO[22], to improve the quality of health care. The CVA-chain allows for the participation of only the general practitioner and the home care. However, larger chain participation is an option as well, e.g. the same patient may be treated by a general practitioner, a neurologist, a rehabilitation centre, a speech-trainer, an ergotherapist, a nursing-home, and the home care. Before addressing in section 5 the specific legal issues that arise in health care chains, the following section first briefly introduces the relevant parties. For, rights and obligations will always be attributed to parties and these rights and obligations will differ considering the their position.

4.4. Relevant Parties

4.4.1 Introduction

Clearly numerous parties may have a role within a health care chain. The type of parties involved will depend on the specific context (e.g. disease).

The picture shows some examples of participants in health care chains. Many others may of course be considered as well. An exploration of the legal position of each of the possible partners within a health care chain is outside the limits of this position paper. Thus, the legal discussion will not be based on each specific participant within a chain (hospital, insurance company, general practitioner, etcetera). Instead and in order to structure the analyses, a distinction will be made between three types of parties:

- the supplier of data;
- the applicant of data;
- the patient.

As will become clear, the applicable rules and regulation will be highly determined by the characteristics of these three types of positions. This section 4.4 aims to introduce some general conditions that are of relevance for the position of the three types of parties. Section 5 will subsequently discuss the implications of the applicable legal regimes.

4.4.2 Supplier of the data

A key question that has to be addressed when considering information flows within chains is who may supply data to other actors within the chain and under what conditions? The answer to these questions is directly related to privacy and the boundaries set on the use of personal data. The relevant criteria to be taken into consideration here are laid down in the Civil Code, by the Medical Treatment Act (Wgbo). For the accessibility and availability of patient data, and respecting the right to privacy of the patient, the supplier of the patient data should comply with several conditions:

1. the health care professional who supplies the patient data should be able to prove that he is

[20] NICTIZ, Architectuurontwerp Basis Infrastructuur in de Zorg. Leidschendam, december 2002.
[21] CVA means Cerebro Vasculair Accident, also known as a stroke.
[22] The project is called: 'CVA Ketenzorg', and is a 'Doorbraakproject' by the CBO: Kwaliteitsinstituut voor de Gezondheidszorg.

currently treating this patient, and he should act in the interest of the patient.
2. The health care professional is responsible for a well organized patient record, that contains the patient data or a specific data set, that is available for the applicant of the patient data.
3. The (electronic) patient record should be organized according to the guidelines of the professional organization of the health care professional.
4. To supply the patient data to the applicants, like other health care professionals, who are directly concerned with the treatment of the patient, the supplier does not need the consent of the patient, as far as the supplied data are necessary for the treatment by the applicant. The patient's consent is neither needed for the disclosure of patient data to the locum tenens (the deputy) of the supplier.
5. The supplier is able to limit the access to the patient data, but is not able to extend the access.
6. The disclosures of patient data by the supplier will be logged.

The criteria appear rather straightforward. However, an evaluation of this Act[23] showed that health care professionals have difficulties in interpreting the criteria for supplying patient data to others. For example, professionals indicated they had troubles in determining when the applicant of the patient data is *directly concerned* with the treatment of the patient, or to interpret beforehand whether the patient data are *necessary* for the applicant to be able to deliver good medical treatment to his patient.

4.4.3 Applicant of the data

Once it has become clear that certain medical data may be supplied to other parties in the medical chain, a subsequent question is how and under what conditions it is sufficiently clear that the applicant of the data is indeed authorized to receive such data. In particular with the introduction of ICT within chains, authorization and identification (management) become crucial issues. The Dutch institute for IT in health care (NICTIZ) indicated that the authorization problem is of key importance in realizing an optimal and safe exchange of data between suppliers of the patient data, applicants of such data and patients.

The present developments in the health care domain indicate towards an authorization scheme of accessing patient data along the following lines. The applicant of the patient data wishes to have access to certain medical data related to his patient, for example the result of a laboratory research, because this information is of importance for the medical treatment of his patient. The applicant provides the patient idenfication number (Zorg Identificatie Nummer: ZIN), his UZI-certificate for health care professionals (Unieke Zorgverleners Identificatie: UZI), and provides what data he wants in particular. Before the data are supplied, a three step approach is required.

The first step is to check whether the patient has consented to the use of the network. It will be possible to verify this in the (national) ZIN-register. In case it is registered in the ZIN-register, that the patient has consented to the use of the network, the second step is to check whether it is allowed for the applicant to have access to the patient data, taking into account his role and the kind of data he applied for. This check will be made by the authorization protocol, which is an important element of the IT-infrastructure in health care. Finally, the third step is to verify whether the applicant has the permission from the supplier of the patient data to have access to the patient data. The health care professional who supplies for the patient data can make his decision personally, with or without consulting the patient, or he may rely on an automated decision. Clearly, these steps should be in compliance with the laws and regulations, especially the Civil Code (Wgbo). This implies for example that (based on the provisions dealing with security) that technical and organizational measures should be taken, such as logging procedures, to control the adherence to the laws and regulations. Given the specific position of an applicant of medical data in a chain, the relevant rules included the Civil Code determine that the following conditions must be complied with by an applicant:

a) When he receives his UZI-certificate, the health care professional has to sign an agreement that says at least that he will not apply for patient data from an Electronic Patient Record, from patients with whom he is not directly involved with given a treatment procedure. The health care professional should also declare that he will not apply more patient data than those that are necessary for a good medical treatment of the patient.
b) The applicant of the patient data should be registered at the national UZI-register (Unique Health care professional Identification register). This register is currently under construction by the CIBG[24], by order of the department of Health, Welfare and Sport and NICTIZ.
c) The identity of the applicant of the data and the authenticity of the application form is known through the UZI-register, and logged. Logging makes it possible to check both the identity and the authenticity.
d) Except the identity of the applicant and the authenticity of the application form, the role of the applicant (doctor, nurse, pharmacist, physiotherapist,

[23] J.C.J. Dute, e.a., *Evaluatie Wet op de geneeskundige behandelingsovereenkomst.* Den Haag: ZorgOnderzoek Nederland, september 2000. Reeks evaluatie regelgeving: Deel 3.

[24] Central Information center for Professionals in Health care (Centraal Informatiepunt Beroepen in de Gezondheidszorg).

etcetera) will also be known, as well as the data (set) that he is asking for.

e) The applicant can use the emergency procedure in an emergency case, when the procedure explained above cannot be followed. Use of the emergency procedure should also be verifiable afterwards. Therefore, logging of the emergency procedures is necessary.

4.4.4 The patient

Accessibility and availability of patient data for health care professionals should in the end be in the interest of the patient. Nevertheless, the processing and sharing activities within a chain with the aim of realising transparency must be in compliance with the laws and regulations. The resulting limitations to processing and sharing activities are also in the interest of the patient, more particular in the interest of the patient's right to privacy and to his right to secrecy. Hence, when considering the patient's position within a chain, again several starting points can be formulated with regard to the access and use of patient data.

a) The patient should be able to give or withhold his consent for the disclosure of his patient data in the health care chain.
b) Health care providers need to comply with the patient's rights, like the right to access his own data, the right to a copy of his own data, the right to delete, supplement, and block his patient data, and the right to secrecy of his patient data.[25]
c) According to the Civil Code (Wgbo), the patient is accorded rights as well as obligations. Examples are the obligation to inform the health care professional, and the obligation to co-operate with the health care professional.
d) The patient, the supplier of the patient data, and a (to be established) supervisory authority, should be able to trace who have had access to the patient data, and what data (set) have been accessed. This tracing can be realized by means of a public terminal or pillar, by a supervisory authority, or through a website, etcetera.

4.5 Legal Issues

4.5.1 Introduction

Given the nature of the data that is transmitted through health care chains, a first key legal regime that determines the limits of and conditions for transparency is privacy. Transparency in health care chains in particular has to comply with the Personal Data Protection Act (Wet bescherming persoonsgegevens, Wbp) and with the Medical Treatment Act (Wet geneeskundige behandelingsovereenkomst, Wgbo) that is incorporated in book 7 of the Dutch Civil Code. Additional legal issues relate to intellectual property rights, especially rights and ownership of databases with patient data. As will become clear, the interaction between data protection law and database law gives rise to several questions. For example, the controller of the patient data, as being defined in the Personal Data Protection Act, may not automatically be the same party as the owner of a database, as defined in the Database Act (Databankenwet, Dw).

Attention must also be drawn to legal aspects that are less related to the *content* itself of the health care chain, i.e. especially patient data, but deal with the legal conditions concerning the *process* of transparency in health care chains. Of particular importance here are liability and evidential issues. In light of these issues, attention will also be given to security, identity management, digital signatures, and the legal status of Trusted Third Parties.

These legal issues refer to the law as guiding principles for social acting and handling, but the law also creates possibilities, as we will see, for social parties to use the law as an instrument, e.g. by concluding a contract. Parties may use a contact to determine their specific rights and obligations (as regards ownership of data, responsibility for data processing, etcetera). Finally, the law creates the possibility, and sometimes the obligation, for technology to complement with legal conditions as well as contractual clauses.

4.5.2 Data protection issues

The earlier-mentioned Personal Data Protection Act (Wet bescherming persoonsgegevens, Wbp), implements into Duth law the European Directive on the protection of personal data.[26] The Wbp specifies various conditions for the lawful processing of personal data in general, and for the processing of special categories of personal data, like medical data. Among the key conditions are (1) personal data may only be collected for specific, explicitly defined and legitimate purposes, (2) personal data may only be processed on one or more of the legitimate grounds, mentioned in article 8 Wbp, and (3) personal data may not be further processed in a way incompatible with the purposes for which they have been obtained (finality principle).

The processing of special categories of personal data, like personal data concerning a person's health, is in general prohibited. However, exemptions to the prohibition of the processing of personal data concerning someone's health are provided in article 21 and 23 Wbp. Whereas the Wbp sets the general conditions for the use of personal data, the Medical Treatment Act (Wet geneeskundige behandelingsovereenkomst, Wgbo), being a special law supplements these general rules with specific conditions that apply to medical data. Both laws are complementary to eachother. The Medical Treatment Act has been implemented in the Dutch Civil Code to strengthen patient's rights in general. One of these patient's rights is the right to protect his patient data. The Medical Treatment Act forces the health care professional to

[25] The right to secrecy of patient data is a right for the patient, but an obligation for the health care professional.

[26] Directive 95/46/EC.

respect the medical secrecy. Within the specific context of a medical treatment, the Medical Treatment Act is applicable. However, the Personal Data Protection Act becomes especially important within health care chains, when patient data are being shared with others.

Given the specific position of a supplier of data, it is important to note that the Wbp requires that a party is responsible for the processing (and thus transmission to other parties in a chain) of personal data. According to the Personal Data Protection Act there should always be one (or more) controller(s) responsible for the processing of the personal data.
As regards the position of the patient, the Wbp requires that the processing of personal data is transparent to patients, i.e. that they are informed of such processing and the underlying reasons. Transparency is among others important in light of the patient's rights to object to the disclosure of their patient data within a health care chain. From the perspective of transparency for patients, the following legal issues need to be considered:

- the patient needs to be well *informed* about the processing of his patient data in general and
- the patient needs to be *informed in more detail* about the access to his patient data in particular.

These two issues are elements of transparency for the patient. Furthermore, in some cases:

- the patient's *consent* is needed before patient data can be supplied to applicants in the chain;
- in certain situations, a patient has a right to *object* to the disclosure of his patient data to other parties in the chain (thus limiting chain transparency);
- the patient should have effective *instruments to control and enforce* the fair and lawful access to his patient data.

When considering transparency within the chain itself (i.e. to the various health care professionals in the chain), mention must be made of the well-knows principle of medical secrecy. According to article 7:457 BW, every health care provider has a binding duty of medical secrecy. Therefore, a supplier is in principle not allowed to disclose any information about his patients to a third party. A third party is anyone but the patient or the health care provider himself. Another health care professional must be considered as a third party. The very existence of this rule appears to hinder any data transmission within a chain. There are, however, several exceptions to the obligation of secrecy. First, disclosure of patient data is allowed when the patient has given his consent (verbally or in writing) for the disclosure.
Second, sharing patient data is allowed when the supplier is subject to a legal obligation. An example of such a legal obligation is article 4 of the Infectious Disease Act (Infectieziektenwet).
Third, certain applicants within the chain do not qualify as third parties, meaning that the supplier can disclose patient data to them without the patient's consent. Applicants that are not regarded to be a third party are among other those who are directly concerned with the medical treatment of the patient, the administrator of the patient records, those concerned with the financial issues surrounding the medical treatment. The supplier is allowed to disclose patient data with these applicants, that are not considered as a third party, but only if the disclosure is necessary, i.e. that the applicants *need-to-know* the patient data. Moreover, the patient has the right to object to the disclosure of his patient data to these applicants.
Fourth, the supplier is obliged to supply the patient data to the patient himself, in the context of his right to access to his own data. The 'medical exception' is not valid to refuse the patient's request for access to his own data. Also, the legal representatives of the patient are not considered as a third party. These representatives are, for example, the parents, the guardian, the trustee, the mentor, the child, the brother, the sister, or the deputy of the patient. For the disclosure of patient data to these persons, the patient's consent is not needed, provided that they act as the patient's representatives.

In conclusion, when considering whether and to what extent patient data may be distributed within chains, both the supplier of patient data as well as the applicant need to consider various issues. The following are of key importance:

- the applicant requesting for patient data has to be directly *concerned* in the treatment of the patient,
- it must be *necessary* for the applicant to have the disposal of the patient data, and
- the applicant has to be *authorized* to have access to the patient data.

The supplier of the data on his side, needs to consider:

- does he need to have the patient's *consent* for the disclosure of the data, or
- is he subject to a *legal obligation* to disclose the patient data.
- is the applicant directly *concerned* with the treatment of the patient.

4.5.3 Intellectual property issues
Copyright law provides that the author or creator or publisher of, mostly a literary or artistic 'work', who owns and provides the 'work', are in principle holders of the corresponding intellectual property rights. The purpose of intellectual property rights is to stimulate the development of works of art, by protecting these works against unlawful and unfair use by others.

Copyright law and database law are of relevance in health care chains because they determine the conditions under which data may be copied, published, extracted and reused. A protected work, like a document or a patient database, may be transacted, accessed, copied, or

transformed. Given the fact that various parties participate in the health care chain, and are thus potentially involved in the establishment of, for example, a patient database, different parties may become right holders to the different variations and formats in which a patient database is available. For example, the patient's administrative data in a centralized patient database can be altered by an employee of one of the participating hospitals, while these data were originally stored into the database by an employee in another hospital. Neither one of these hospitals may, however, be the sole rightholder of the patient database. This means that the various participating parties within the health care chain, that use the patient database, should take careful consideration of the fact whether they want to determine their respective rights to use of the data by means of contractual clauses. A contract between the different parties (in their position as suppliers of data and applicants, i.e. users of data) may thus stipulate the various rights and responsibilities of the partners in the centralized patient database. Technology can complement the legislative and contractual provisions in that it embeds control flags indicating whether accessing, copying, altering, updating, and deleting of patient data is authorized.

Special attention should be given here to the legal status of databases, since they are crucial information sources in chains and questions thus arise who owns a database and what rights can be based on such ownership. For example, an existing example of a regional health care network in the south-west of the Netherlands, uses a centralized patient database that contains the administrative data of patients that are registered by one of the participating hospitals. These administrative data are shared with and administered by all participating hospitals. These hospitals have outsourced the processing of this patient database to a processor. Under the rather new legal phenomenon of database protection[27], the titleholder to the database is the producer (the maker) of the database, i.e. the one who substantially invested in the database. The owner may thus be another actor than the one who actually collected or selected the data. The situation is different when there is an engagement, or co-operation, or the work has been created under guidance and surveillance. The owner of the *sui generis* right can, therefore, be another than the owner of the copyright. He may also be another than the controller of the patient data.[28] In other words, the different parties operating in a chain and aiming at enhancing transparency of information relations within this chain, need to be aware of the different regimes (data protection, copyright and database law) that apply and all accord different rights and responsibilities to the parties.

[27] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. The Directive has been implemented in the Dutch Database Act (Databankenwet, Dw) in 1999

[28] See also M. de Koning, H.H. de Vries, Databankenrecht en privacyrecht. *Privacy & Informatie*, 2003, nr. 2, p. 52-59.

At this point it is of relevance to return to the legal regime on personal data protection (privacy), because there appears some friction between this regime and the database protection regime (intellectual property). Although article 13 of the Database Directive provides that the legal protection of databases is without prejudice of other legal provisions, such as rights related to, for example, data protection and privacy, practice shows that uncertainty exists as regards the position of the different parties with respect to databases and the data included therein.

The organization responsible for the use (processing) of personal data is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of the personal data. The term used for this person under the law is 'controller'. Although the controller may turn out to be the same party as the owner of the database, this is not always the case. The controller determines the purposes and means of the processing, but this does not exclude the possibility that another actor provides the financial means and therefore delivers the substantial investment. Thus, an actor in the chain may qualify under the data protection law as 'controller' and thus be responsible for the information in the database, but he cannot claim to be the titleholder (owner) of the database under database law. Here the strange situation arises that according to the Personal Data Protection Act, it is not possible to process personal data without qualifying as a controller. It seems impossible, that the owner of a database can carry out his exclusive right, without *de facto* process personal data in his database. He may, for example, want to update the database. Any updating of personal data is considered to be a kind of processing. Therefore, it seems that the owner of the database is always the controller of the processing of the personal data.

Nevertheless, it seems possible that the criteria of the Personal Data Protection Act and the Database Act, can be complied with in a different way. The owner of a database can delegate the role of the controller to another party. This is possible by concluding a contract. The contract, however, shall be without prejudice to the compliance with the Personal Data Protection Act. The

Personal Data Protection Act is coercive, which means that it is not allowed to depart from the legal obligations by a contract.

On the other hand, it seems also possible that the controller respects the ownership of the database by another party, because this third party has provided the substantial investment. The owner of the database may, for example, not be able to refer to one of the conditions for legitimate processing. In this case, the parties should conclude a contract in which they stipulate that the owner guarantees that the controller will be able to comply with his obligations according to the Personal Data Protection Act.

In brief, the maker of a database is the person who takes the initiative and the risk of investing. In specific situations, the controller, for example a hospital or group of hospitals, may outsource the creation or maintenance of a patient database to a processor. The question arises, who in this situation should be considered as the maker or the author of the database: the hospital(s) or the processor?

When the client, i.e. the controller, is the one who made the investment and runs the risk, he is the client who owns the ownership rights to the database. However, co-ownership may also be the case, for example when the controller and the processor both invested in the database. In such cases it is preferable to conclude a contract in which the database right is put into one hand. In other words, to guarantee that the responsibilities of the different partners within a chain are clear and sufficiently determined, a contractual arrangement between these parties seems indispensable. Without contractual arrangements the protection of databases, and the protection of personal data might erode, leaving the parties within the chain with legal uncertainty as regards their position.

4.5.4 Liability

A third legal domain that is to be addressed is liability. In health care chains, health care professionals are liable for non-compliance with their legal obligation to medical secrecy. The health care professional can be held liable for breaching his professional secrecy in disciplinary law, civil law, and criminal law (breach of professional secrecy is punishable according to article 272 Penal Code, WvSr). The Medical Treatment Act provides for a centralized liability for the hospital (article 7:462 BW). This means, that when a patient wants to start a legal procedure against a health care professional, who is working in a hospital, the patient can charge the hospital. Therefore, there are little or no possibilities to arrange liability by contract. In general, the hospital has a right to recourse against the health care professional.

In light of the responsibilities of the various parties and thus the liability for their dealings with data, mention must also be made of the obligation under the Personal Data Protection Act to conclude a contract between the parties involved in the processing of personal data. For example in case a hospital outsources the processing of the administrative data to a third party, both are obliged to conclude a contract in which they specify certain issues (such as the security measures taken when the data are transmitted between these actors).[29] In case one of the parties fails to act according to the provisions of the contract, this party will be held liable.[30]

Liability may arise in other chain-related situations as well. Data that are transmitted through chains and thus are being handled by various parties, are vulnerable for becoming incorrect. Here, the parties in the chain must consider the consequences of such possible incorrectness under liability rules. Incorrect patient data can lead to serious physical harm for a patient, because the health care professional founds his treatment on them. Although hospitals are normally considered as the controller or patient data, as defined in the Personal Data Protection Act, the health care professional himself remains responsible for the quality of the patient data. In other words, all relevant actors in the chain will share a part of the liability risk and – in legal terms - the liability for patient data is thus based on a system of scaled liability. It thus appears of utmost importance that all parties in a chain determine what can be expected from themselves to secure the correctness of the data (security measures, use of protocols, use of authentication and verification measures, etcetera) and who bears to what extent the burden of liability in case something goes wrong. Also, parties in the chain have to introduce some sort of organizational and technical measures to trace at what moment and why things went wrong. Such a 'trail' will be of importance in case a dispute arises between the parties and proof must be handed what actually happened and under whose responsibility. This leads to the final legal issue to be discussed here: evidential value of documents, electronic files, agreements, etcetera generated by means of the dealings of parties within a chain.

4.5.5 Evidence

Practice shows that patient data in patient records are becoming more important to provide evidence in lawsuits.[31] The general evidence rule is 'who claims, must prove'.[32] This means that a plaintiff who refers to certain

[29] For a more detailed discussion of the possible contractual clauses, see: College Bescherming Persoonsgegevens, *Privacy Audit Framework under the new Dutch Data Protection Act (WBP)*. Report by the Co-operation Group Audit Strategy, version 1, April 2001, p. 52.

[30] Liability for the use of personal data is also regulated in the Personal Data Protection Act. Article 49 Wbp establishes a right to compensation when personal data have been used in conflict with the provisions in the Personal Data Protection Act. Compensation can be provided for material and immaterial damage. It is also possible to claim a judicial prohibition to prevent further acting in conflict with the law.

[31] See J. Legemaate, *Goed recht. De betekenis en de gevolgen van het recht voor de praktijk van de hulpverlening.* Preadvies uitgebracht ten behoeve van de jaarvergadering van de Vereniging voor Gezondheidsrecht op 22 april 1994, p. 63-75.

[32] Article 150, Civil Procedure Act (Wetboek van Burgerlijke Rechtsvordering).

facts or certain rights, has the burden of proof. For evidential reasons it is important for health care professionals to keep record of patient data. A patient record can play an important evidential role in disciplinary or civil procedures. Security in health care chains, more specifically data integrity and availability of patient data, is therefore also of importance for evidential reasons. Most of all, the quality of patient records is important for the quality and continuity of health care, and for the accountability for and control of medical treatment. Also, the issuance of certificates and electronic identification schemes (such as digital signatures) appear important instruments.

The UZI-certificate, that has been mentioned earlier, will provide the health care professional with a digital signature. User identification and authentication by the UZI-certificate is part of the architecture for on-line identity management. Of course a prime question that is raised here relates to the legal status and thus evidential value of digital signatures and the position of certification authorities. Legal uncertainty as to the status of digital signatures can be an obstacle to the implementation of a basic infrastructure for health care incorporating digital signatures. Contractual solutions between the partners in a health care chain cannot remove these legal impediments completely. Therefore, digital and electronic signature legislation and regulations concerning related matters have been adopted by different countries, international organizations and the European Union in order to meet the expectations and needs of the digital market in light of legal certainty. Currently, the Dutch Digital Signature Bill is awaiting its final approval by the First Chamber. Under the new legal rules, security parameters indicating authentication, confidentiality, data integrity, and non-repudiation service levels along the health care chains, remain of utmost importance. Hence, such parameters should be addressed while contemplating the architecture and model for on-line identity management.

Having discussed several legal issues from a more general perspective, attention must subsequently be given how the two most relevant legal issues (personal data protection and database protection) work out for the three types of parties that have been introduced earlier. For the exact status of a legal rule highly depends on the specific circumstances of the situation involved. Thus, only by discussing the two key legal domains in their specific context (i.e. the context of a party), can a clear picture be drawn of the problems that arise when considering the interaction between law and chain transparency.

5. CONCLUSIONS AND DISCUSSION

In this paper we have seen that seen from a legal angle, transparency in network chains comes in different guises. Transparency can be private – for use of the parties in the network chain only, or public – also for the general public and the authorities. It can be based on legislation or on self-regulation and even on enforced self-regulation. It can be provided voluntarily or to fulfil a legal obligation. It can even be enforced by public authorities. The different guises raise different legal questions.
The example of the food chain raises several legal questions. On the one hand it shows that even in a legal environment that is friendly to transparency in the chain, much information that should have been passed on can get lost or distorted. This raises the question on the responsibility and liability for incorrect information. To what extent can provisions be made for it to be passed on upstream to the company that made the initial mistake?
Another question that comes up in the context of the legal obligation to share information is how (innovations in) composition of foodstuffs and inter-company relations can be protected.
A final question relates to the position of consumers within food chains. In scientific and legal literature only few thoughts have been given to the question whether and how the legal position of consumers in such chains can be strengthened.

The health care chain analysed in section 4 shows that there are at least four legal domains that raise questions and uncertainties.
The first legal domain relates to *accountability*. Within the context of health care chains, the issue of accountability raises several questions. A glance at the data protection law shows that uncertainty may exist as regards the question who the 'controller' is, as defined in the Wbp. Given the fact that several actors may be involved within a particular health care chain, parties must clearly determine which actor qualifies as the 'controller'. It may happen that more than one actor qualifies as the controller.

The second legal issue is about *ownership*. Uncertainty exists with regard to the ownership of patient data, and of the database containing patient data. According to the current doctrine, there is not one party who can be considered the owner of patient data. The hospital, health care professional, and the patient all have certain rights and obligations with regard to the patient data. All three of these actors have some kind of authority over the patient data. The maker of a database is normally considered to be the owner of the database. The owner of the database is the party who substantially invested in the database. The owner may, therefore, be another party than the one who actually collected or selected the data. Also, the owner may turn out to be a different actor in the chain than the 'controller' of the data under the data protection law.

The third legal issue relates to *transparency*. As discussed, transparency in health care chains has at least two possible meanings. First, transparency deals with openness for the data subject, i.e. the patient. The patient must be well informed about the processing of his patient

data, in particular with regard to the sharing of his patient data within the health care network. The second dimension of transparency sees to transparency within the chain (i.e. between the different health care service providers). Health care professionals who share data about their patients with other health care professionals, need to realize that only under certain conditions they are allowed to breach their professional secrecy. Respecting this medical secrecy, procedures should be developed to ascertain that the applying health care professional is authorized to have access to the patient data. In general, access is only permitted with the informed consent of the patient. In this respect, it makes a difference whether access is authorized within the health care chain, or the patient data are disclosed to a third party, outside the health care chain.

The fourth legal issue deals with *security*. Here several perspectives apply. Security of information and information systems is of importance for the confidentiality of the information, the integrity of the information, and for the availability of the information. The confidentiality of information can, for example, be secured by regulating the access to patient data by technical and organizational measures. These measures also need to secure the integrity of the information. They have to prevent that patient data are not accidentally or unlawfully deleted, or altered, or unauthorized disclosed or accessed. These measures should guarantee that patient data are correct, complete and up-to-date. Finally, security measures must ensure the availability of information. The availability of information is important, for example, for the quality of health care, but also for evidential purposes. Within electronic network environments, especially when sensitive personal data are being processed, it is important to strengthen the value of electronic evidence. Electronic evidence can, for example, be strengthened by means of an independent authority, a Trusted Third Party. A Trusted Third Party can act as a Certification Authority, which certifies encryption keys for digital signatures. Digital signatures can also be used for time stamping: the Trusted Third Party places his own digital signature in the electronic document, adding date and time. The Trusted Third Party declares that the electronic document did exist at that time and in that state.

In all four domains various issues need further clarification in order to enhance an adequate and lawful transparency within health care chains. Such clarification can to a large extent be realised by the chain partners themselves (e.g. by means of contractual agreements, technical and organizational measures). There are however also some new issues that need further research. We mention the following by way of example.

Large databases created once various parties start cooperation and exchanging information within chains, allow for the application of new processes and dealings with patient data. A large potential is expected from so-called data mining applications. Patient data can also be subject of statistical analysis and scientific research. The question arises, what conditions must apply when parties within a chain are in principle given the ability to generate whole new data from available database by means of data mining? What types of use are allowed, and what not? Does the patient need to be informed about this? One of the key challenges here is that data and patient profiles generated by means of data mining does not fall within the ambit of data protection law (because these data often say something about a group of persons instead of an individual). What criteria for fair and lawful processing of such data should be applied?

Another new legal issue deals with the conditions for anonymization. It may be doubtful whether identification should always be the starting point in health care chains. By using Privacy Enhancing Technologies, it is possible to process a patient's administrative data and his medical data in different databases, separated by an identity protector. Identity management should also pay attention to pseudo identities in health care chains. A working example of PET, using an identity protector, is developed at the Dutch mental hospital, De Meerkanten.[33]
A final issue deals with the fading boundaries between public and private interests. Clearly, patient data generated within health care chains, are of potential interest for private organisations, like health insurance companies. Given the growing number of public activities performed by private organisations, questions may arise as to in whose interest transparency of patient data actually is.

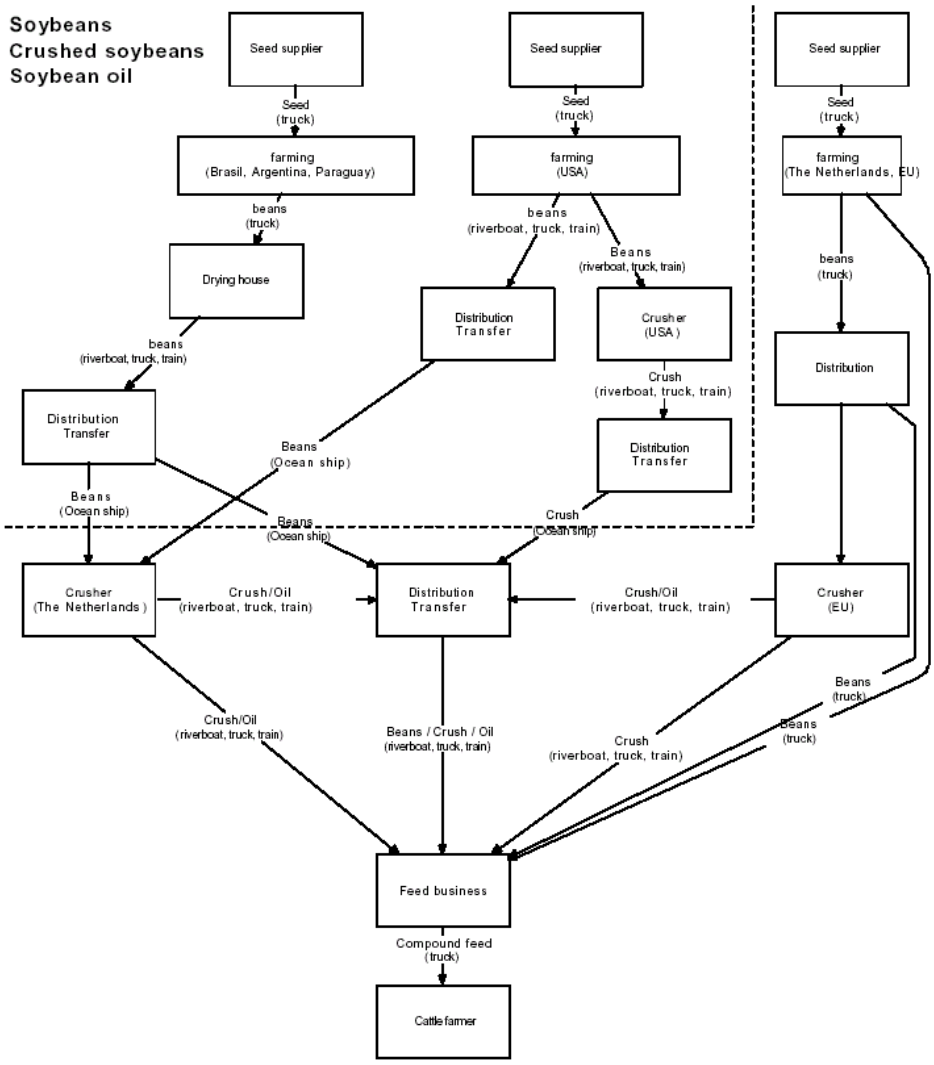
This position paper started with the observation that balancing the interest of possession and ownership of information on the one hand and the interest of access and general availability of information on the other hand will be one of the key challenges in our information society. Both interests have clear foundations in specific legal regimes and the relevant provisions aim to establish – given a certain context – a situation in which both interests interrelate.
A glance at the interaction between law and chain transparency in two specific chains shows that many of the issues discussed relate to the question "to what extent and under what conditions do the interests of the various parties involved indeed require that transparency is aimed for?" We noted with respect to the food chain that transparency and thus sharing information may conflict with the interest of protecting (innovations in) composition of foodstuffs and inter-company relations. In the health care chain the tension is clearly visible in a patient's right to personal data protection and a health care professional's duty of secrecy. A clear and ultimate answer on where exactly the borderline must be set when balancing transparency interests in chains against personal

[33] G.W. van Blarkom RE, Meer kanten aan PET: PET in de praktijk bij Meerkanten. *Privacy & Informatie*, 2002, nr. 5, p. 210-216.

(property) interests cannot be given here. What can be said is that all partners in chains must realise that transparency and thus sharing data and information is not and cannot be a goal in itself. Creating chains and working together in chains implies that the participating parties take careful notice of the interests of their chain partners as well as the rights accorded to these partners under the law. As said, many of the issues that subsequently need to be cleared can be addressed by means of contractual provisions. This does not mean that it will be simple to draft such provisions. Further research needs to be conducted what provisions can be made for issues such as liability, confidentiality, ownerships, etcetera.

In addition, many new challenging issues arise and need full attention in light of the potential of chain development as well as transparency within chains. Many of these new challenges relate to fundamental dilemma's with respect to ownership of, access to and fair dealing with information in chains.

Annex 1 Soj feed chain



From:
C.W.G. Wolf, M.W. Hoogeveen and J.J. de Vlieger, Ggo-vrije veevoedergrondstoffen voor de melkveehouderij, Borging, beschikbaarheid en kosten, LEI 2003.