出國報告（出國類別：考察）

丹麥、挪威保險對象個人資料比對及對外提供之管理機制

服務機關：行政院衛生署中央健康保險局
姓名職稱：王怡人組長、王復中科長
派赴國家：丹麥、挪威
出國期間：99 年 8 月 21 日至 99 年 8 月 29 日
報告日期：99 年 11 月 26 日

摘　　要

透過實地參訪考察國外相關機構對健康（保險）資料的蒐集、處理、比對串接原則、個人資料保護法令規範以及研究資料提供方式等，可做爲「全民健康保險研究資料庫」運作執行及檢討本局對外資料提供機制之參考。

本考察報告除說明所考察各機構的內容與心得外，也在個人健康（保險）資料比對、對外提供之法制與技術面管理議題提出建議，期望能爲後續政策與執行規劃提供具體的建言及貢獻。

目　　次

丹麥、挪威保險對象個人資料比對及對外提供之管理機制

壹、 緣起與目的

全民健康保險開辦至今已超過15年，收載了豐富的民眾投退保資料及特約醫療院所費用申報資料，是台灣醫藥衛生研究重要的實證資料。為促進健保等相關領域之研究，行政院衛生署中央健康保險局(以下簡稱本局)自2000年起委託財團法人國家衛生研究院(以下簡稱國衛院)建置與管理「全民健康保險研究資料庫」，負責對外提供全民健保學術研究資料加值服務，該院並於今年(2010年)起，開始以現場作業(On-Site)方式，提供健保資料與死因資料比對服務。由於全民健保研究資料庫內容包含個人資料，本局在資料交付國衛院時，即已進行個人識別資料加密，該院管理上除透過隱名化(Anonymous)及資料再加密來確保個人隱私，也要求使用者必須遵守保密切結規定。

如何兼顧資料安全與保護個人隱私及促進學術研究，一直是本局與國衛院努力的重要課題。尤其今年通過的個人資料保護法中，不但對強化對個人資料的保障，也對醫療資料的蒐集、處理或利用有更嚴謹的規定。未來公務機關或研究機構為學術研究所為的醫療資料蒐集、處理或利用，將由行政院衛生署會同法務部定訂辦法規範資料範圍、程序及其他應遵行事項。而目前行政院研考會整理「總統政見執行追蹤一覽表」之「16.人權政策」內容中，也提到政府資料庫不得恣意聯結、濫用個人資料、侵害人民隱私之政策指示。因此，本局有必要瞭解先進國家作法是否有值得借鏡之處，以因應未來環境發展趨勢，並做為改善保護資料安全與個人隱私及促進學術研究之參考。

世界先進國家對於公部門資訊或資料之提供，均有相當嚴謹的規範，以保障民眾個人隱私。經蒐集並分析各國相關資料後發現，丹麥自1968年即建立CPR(Center Population Register)系統，開始透過個人辨識資料(Personal Identification Number)來協助各資料庫間的資料比對，提供政策分析或學術研究使用，該國於2000年5月通過個人資料處理法案(Act on Processing of Personal Data)後，對全國民眾的社經、健康等資料，不但有完整的保護與管理機制，也能透過專責機構提供

學術研究所需的資料與資料串接服務，運作良好並獲致相當成果；另一方面，挪威政府對於如何有效運用健康資料促進學術研究，已有多年成功經驗，該國的健康資料服務提供機構聲譽卓著且已朝向國際化發展，也相當值得借鏡。因此，本局規劃此次考察活動，以實地瞭解學習丹麥、挪威兩國在健康資料比對及對外提供上，相關的運作機制、作業規範及個人資料保護等議題，並希望藉由此次的交流，帶回寶貴經驗，做爲未來業務推動及持續改進之參考。

本次考察主要目的如下：

(一) 個人資料比對之法律規範、作業原則。

(二) 研究資料對外提供之運作、管理機制。

貳、 過程與內容

爲執行本考察案，經洽詢丹麥、挪威各相關機構，聯繫考察之可行性，獲丹麥健康資料主管機關 Danish National Board of Health、負責國家統計資料製作及研究資料提供的 Statistics Denmark、研究資料使用主管機關 Danish Data Protection Agency，以及挪威負責疾病預防、健康研究與對外研究資料提供的 Norwegian Institute of Public Health、該國最知名的社會科學研究資料服務公司 Norwegian Social Science Services 等共五個機構同意，考察過程與內容分述如后。

一、參訪機構及過程

本次考察包括交通往返時間共計九日，各機構參訪安排時間如下：

8/23 (一)：考察 Danish National Board of Health 及 Statistics Denmark

8/24 (二)：考察 Danish Data Protection Agency

8/25 (三)：考察 Norwegian Institute of Public Health

8/25 (五)：考察 Norwegian Social Science Data Services

各機構之地址、接待主管與連絡人員如詳附錄一。由於這些參訪機構對本局

來訪均相當重視，除行前多次溝通討論考察議題外，當天均準備簡報，爲本局參訪同仁提供詳盡的說明，並回答相關問題。各機構之簡介說明如下：

(一) Danish National Board of Health

該機構成立於 1906 年，隸屬內政與衛生部(2010 年改制，原爲衛生部)，目前員工約 400 人。其主要工作爲：監測全國健康狀況、對內政與衛生部及其他機構提出建議、醫療從業人員的咨詢與管理等，而有關全國性健康資料收集工作亦屬於 National Board of Health 的工作範圍，由其負責健康資料庫之維護、管理與統計。該機構英文名稱雖有「Board」，事實上組織架構中並無委員會，本次考察主要接待者爲 Documentation Department 主管 Dorte Hansen Thrige 及其同仁，該部門即爲健康資料之主管單位。

(二) Statistics Denmark

丹麥國家統計局成立於 1850 年，負責丹麥全國統計資料製作及發佈，目前員工約 550 人。2010 年預算約 5000 萬歐元，30%的財源來自營業收入，其他主要由國家經費補助。僅管如此，爲維持統計資料公正客觀，該局係獨立運作，由理事會(The Board of Governors)決定工作目標及工作內容。依據法律規定，丹麥國家統計局可以向政府機關、企業及個人要求提供資料，被要求者不得拒絕，否則會有罰則。除了發佈統計資料外，該局也負責維護研究者使用的資料庫，其資料庫遠比 National Board of Health 所擁有的資料更爲廣泛，除了健康資料，還包括社經、稅務等資料，由於可以進行多資料庫之連結，研究者透過申請，可將就醫資料與教育、就業及收入等資料串接，進行更深入的分析。本次考察主要接待者包括了統計、資訊及 International Consulting 等部門主管，會後也拜會了該局 Chief Adviser of Director General's Staff (類似我國行政機關的主任秘書)Bo Johansen，感謝其促成此次考察活動。

(三) Danish Data Protection Agency

該機構隸屬司法部，員工數約 35 人，並設有 Data Protection Council 委

員會，委員會由學者、法界人士與政府代表共 7 人組成，成員均由司法部指派。基於個人資料處理法案的規定，只要涉及個人資料研究，研究者必須將研究方式、資料處理流程等內容通知 Data Protection Agency，並經該機構同意後，始得向 National Board of Health 等資料提供機構提出使用申請。委員會每年召開 6 到 8 次會議，主要討論個案的原則，再交由 Data Protection Agency 處理。本次考察主要接待者爲該機構主管健康研究之資深顧問 Camilla Daasness 及其同仁。

(四) Norwegian Institute of Public Health

該機構隸屬於挪威健康照護服務部(Ministry of Health and Care Services)，員工數約 900 人，年度預算約 1.6 億美金。Norwegian Institute of Public Health 不但負責疾病預防與國民健康監測，也進行健康研究，提供政策建議及研究資料提供服務。本次考察主要接待者爲該機構 Division of Epidemiology 主管 Per Magnus 及其同仁，該部門除負責流病監控外，也是研究資料、健康統計及 Biobank 的主管單位。

(五) Norwegian Social Science Data Services(NSD)

NSD 成立於 1971 年，一開始爲挪威國家研究委員會(類似我國的國科會)的一個部門，2003 年起改制爲有限公司，隸屬該國教育研究部，爲目前世界最大的幾個研究資料庫暨資料提供服務機構之一。該機構設有委員會(Board of Directors)監督機構運作，委員會成員共 7 人，其中 2 人爲 NSD 員工代表，其他 4 人爲學者，另 1 位則爲挪威國家統計局(Statistics Norway)代表，委員會成員均由教育研究部指派。NSD 員工數約 70 人，年度預算約 4000 萬挪威克朗，主要經費來自國家研究委員會及教育研究部(約佔 1/2)。作爲挪威國家研究資料服務中心，NSD 主要負責協助研究者在資料蒐集、分析、資訊技術及個人隱私方面的問題，以克服其資料使用障礙。NSD 也與其他政府機構合作，包括挪威國家統計局及 Norwegian Data Inspectorate(類似丹麥的 Data Protection Agency)等，詳細內容將在下一節說明。本次考察由 NSD 負責人(Executive Director)Bjorn Henrichsen 親自接待，其他幾位副主管(Deputy Director)也陪同出席。

二、考察內容

(一) 丹麥個人資料比對之法律規範、作業原則

該國個人資料使用最重要的原則，爲 2000 年 5 月通過之個人資料處理法案，規範所有個人資料處理相關事項，其重要條文節錄如附錄二，由法條內容與位階來看，類似於我國的個人資料保護法。此法案係基於歐盟 1995 年 95/46/EC 法案，將個人資料視爲 Human Rights 所制訂，故歐盟其他國家也陸續訂定有類似之法律。

依據上述法案，任何針對個人資料的處理，必須訂定明確且特定的目的，資料處理非經當事人同意或爲促進公共利益，原則上不得作爲目的外的使用。法案中將個人資料可分爲敏感性(Sensitive)及非敏感性(Non-Sensitive)兩類，健康相關資料屬敏感性資料(參閱法案 Section 7)，其內容除了預防保健、醫療診斷處置外，還包括血液樣本等生理辨識資料。非常特別的是，對於這類敏感性資料，法案明定符合統計或科學研究目的使用時，得在可辨識個人的情況下處理運用，而這項特別的規範並未見諸於其他歐盟國家。根據 Data Protection Agency 的說明，訂定這樣的條文有其歷史因素，因爲丹麥很早就允許爲統計或科學研究，主管機關可提供個人身份辨識資料，以供不同來源資料庫進行資料比對串接服務。不過，該法案也規定，任何統計或科學研究處理的結果，不論是否屬敏感性資料，不得再做爲其他用途。這也意味者科學研究的結果是無法用來提供做爲病患的醫療資料，雖然這樣的限制曾受到醫師的抗議，但法案的規定並無任何例外。

依據個人資料處理法案的規定，使用敏感性個人資料時，必須取得 Data Protection Agency 的許可(Notification，詳如法案的第 12~13 章內容)，違反者會有刑罰及罰款。Data Protection Agency 採書面審查，申請者必須說明：(1)資料負責人、(2)資料處理流程、(3)資料儲存方式以及(4)工作完成後，何時銷毀資料等事項。一般的統計或學術許可申請是免費的，

其他如藥廠的科學研究許可申請每件收費 1000 丹麥克朗。基本上，除非申請者透過法庭訴訟，否則 Data Protection Agency 就是資料使用的最後決定機關。爲了確保使用者有按申請目的使用及妥善管理，例如是否有將可識別資料加密或轉換，資料是否有設置存取密碼等，Data Protection Agency 每年均會抽查約 25~30 件許可案件，根據 Data Protection Agency 表示，查核結果顯示過去申請者均有妥善使用管理資料。

獲得 Data Protection Agency 同意的案件會公佈在網站上，使用者獲許可後即可向資料主管機關提出申請，以便取得實際的資料。健康資料主管機關爲 National Board of Health，向其提出申請時，National Board of Health 會先確認該申請是否已獲得 Data Protection Agency 許可，再進行後續的資料庫比對串接及資料提供服務的審查。

(二) 丹麥研究資料對外提供之運作、管理機制

1. National Board of Health 擁有行政管理及研究兩類資料，清單如表 1。National Board of Health 擁有這些資料的主要目的，一方面是爲了監測公眾健康狀況，另一方面就則是用來提供政策規劃及學術研究使用，其外部服務對象除了研究者，還包括民意代表、媒體及一般大眾。如果是隱名化資料，由於不屬個人資料處理法案規範的範疇，並不需要事先經過 Data Protection Agency 許可，故這部分是由 National Board of Health 全權決定。但由於透過個人 ID(CPR-no)，National Board of Health 可以將不同資料進行比對串接，研究者使用這些資料時必須透網路申請，每個申請需要有：(1)研究描述、(2)Data Protection Agency 許可、(3)使用資料的完整描述，如果是調查研究，必須附上問卷，如果研究涉及生理樣本採集，還必須額外取得另一個機構 Danish Council of Ethics 的同意。

   National Board of Health 由 Research Service Unit 負責處理這些申請案件，對於前述的兩類資料，有不同的處理流程：研究類資料庫因爲有高度敏感的個人資料，研究者如果申請這類資料，如 Cancer Registry，Research Service Unit 會再一次將這個申請送給 Data Protection Agency

表 1：Danish National Health Registries

行政管理類資料庫	
The Civil Registration System, CPR-no	1968 啓用
The National Patient Registry	1977 啓用
The Causes of Death Registry	1970 啓用
The Medical Birth Registry	1978 啓用
The Registry of Birth Malformation	1983 啓用
The Register of Legal Induced Abortions	1973 啓用
The National Health Insurance Service Registry	1990 啓用
Authorized Health Personnel Registry	1982 啓用
研究類資料庫	
The Cancer Registry	1943 啓用
The Pathology Registry	1997 啓用
The In Vitro Fertilization Register	1994 啓用
The National Diabetes Registry	1996 啓用
The National Registry of Alcohol Treatment	2006 啓用
The Military Service Liability Registry	2006 啓用
The Central Dental Registry	1972 啓用
The Psychiatric Central Research Register	1969 啓用

審查，經其同意後才能提供；行政管理類資料庫則不用進行這個步驟。根據 National Board of Health 的說明，該機構每年約有 400 件申請案件，一般來說，行政管理類資料約 1 個月可提供，研究類資料由於須再送 Data Protection Agency 審查，約需 2 到 4 個月。該機構提供資料時，只收取資料處理這部分的費用，並以每小時 1200 丹麥克朗計費，此項服務年收入約 200 萬丹麥克朗。

2. 丹麥國家統計局所擁有的資料，除行政管理類資料庫(約 95%)，也有一些透過調查研究得到的資料(約 5%)，該局對於蒐集來的資料，如發現有錯誤時，除非是系統性的問題，否則是不會回饋給原提供機關。這些資料除供內部使用外，有兩種對外提供方式：一是統計資料(Statbank)，目前有丹麥及英文版，任何人都可以透過網路免費存取，每年約有 2 百萬次使用紀錄；另一是明細資料(Micro Data)，只提供政

府機關或研究分析人員申請，獲得同意後，才能使用。所有明細資料均以去除可辨識(De-Identified)方式處理後，存放於局內獨立的電腦環境中，再由原申請使用者透過網際網路連線使用，這些明細資料不能傳送到局外，只有統計結果可透過 e-mail 傳送給使用者。經詢問丹麥國家統計局，這項做法過去是以現場作業方式，由使用者親自至該局內操作，分析完成後將結果攜回，不帶走明細資料，但因場地有限，且現場作業人力成本較高，故該局於 2000 年以後改以透過網際網路連線方式使用至今，目前約有 1200 人申請使用中，每天包括內部使用者約 100 人同時上線使用。

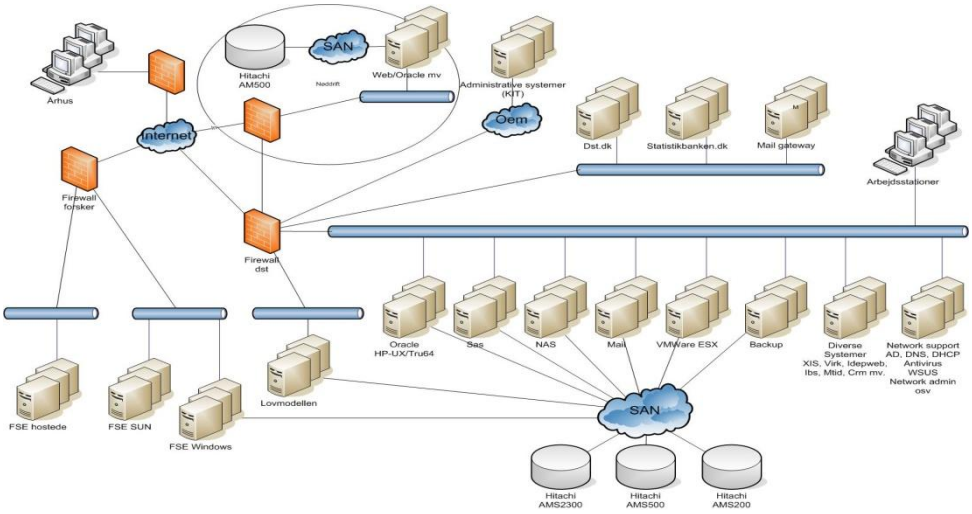


圖 1：Network Overview

由於丹麥國家統計局所擁有資料的廣泛及敏感性，該局對於資料對外提供，比 National Board of Health 有更嚴苛的限制，例如前述所有提供的明細資料都不能辨識出個人或機構、資料須獨立存放並進行加密等。此外，由於透過網際網路使用，爲確保資料安全及可靠性，除設置防火牆外，並採取 Virtual Private Network(VPN)方式連線(如圖 1 所示)，使用紀錄保存 6 個月。根據該局資訊部門主管表示，採取這種作業方式後，除了 10 年前曾有過一次首頁遭駭客入侵被置換外，目前爲止並未發生任何資安問題。有趣的是，只有丹麥國家統計局及合作夥伴被授權人員才可以使用可識別之個人資料，這部分照說必須符

合個人資料處理法案的規定，須要 Data Protection Agency 許可，但由於 Data Protection Agency 對丹麥國家統計局採取較寬鬆的審查，也從不稽核該局，所以該局內部使用可識別之個人資料比較仰賴內部的自我管控機制。

(三) 挪威個人資料比對之法律規範、作業原則

該國個人健康資料的比對及使用，主要由三個法案所共同建構，包括：2000 年 4 月通過之個人資料法案(Personal Data Act)、2001 年 5 月通過的個人健康資料建檔法案(Personal Health Data Filing System Act)以及 2008 年 6 月通過的健康研究法案(The Health Research Act)。與丹麥相同，個人資料法案係基於歐盟 1995 年 95/46/EC 法案所制訂，給予個人資料處理原則性的規範，由於健康資料屬敏感性個人資料(Section 2, no.8)，處理時有較嚴格的法律規範，因此，須透過個人健康資料建檔法案提供資料蒐集處理的法源依據。在這兩個法案的共同規範架構中，健康資料可以在法律授權或取得 Norwegian Data Inspector Agency(獨立機關，類似丹麥的 Data Protection Agency)的許可(Licence)兩種方式下，無須經由當事人的同意，進行健康資料蒐集、處理及使用。而健康研究法則是個很特別的法律，主要規範生物醫學的(Biomedical)研究資料使用，惟這些資料的蒐集、建檔及比對事項，仍依據健康資料建檔法案來處理，故健康資料建檔法案是最核心的法律規範。

健康資料建檔法案條文詳如附錄三，明訂 10 種個人健康資料庫，可以直接蒐集處理，但個人 ID 等辨識資料必須以加密方式儲存在資料庫(Section 8)，只有管控單位(Data Controller)的授權人員(Data Processor)可以進行個人資料比對處理。爲了保護個人隱私及確保資料的正確性，針對這些具有個人辨識資料的資料庫，個人資料法案中規定，管控單位必須事先取得 Data Inspector Agency 許可，Norwegian Institute of Public Health 就是經 Data Inspector Agency 許可的管控單位。

(四) 挪威研究資料對外提供之運作、管理機制

1. Norwegian Institute of Public Health 除了負責全國健康監測、傳染病制等業務，也進行許多研究，法律並給予該機構資料管控權利，該機構也會將持有的資料庫對外提供。然而，法律雖給予 Norwegian Institute of Public Health 收集相關資料的權利，但也要求該機構必須確認資料正確性，這項工作對於擁有很多資料庫的 Norwegian Institute of Public Health 來說，是很大的挑戰。在參訪的過程中，該機構介紹許多不同資料庫及其研究應用，參訪人對 Norwegian Prescription Database(NorPD)及 MoBa(即 Mother&Baby)Biobank 留下較深刻的印象：

(1)NorPD 自 2004 年開始使用，內容包括所有民眾在藥局所交付調劑的藥品，這個資料庫是健康資料建檔法案惟一同意個人辨識資料可不加密儲存的資料庫(Section 8)，讓研究者可以透過病人的 ID 或藥師的 ID 來比對串接其他資料庫，這類研究申請必須先經過 Data Inspector Agency 許可。NorPD 可以進行資料比對串接的原因，與世界衛生組織(WHO)藥物統計方法協同中心設在 Norwegian Institute of Public Health 有關，此資料庫也以隱名化方式提供給一般的研究申請案件使用。

(2)MoBa(即Mother&Baby)爲挪威以懷孕婦女所進行的大型世代研究，根據人口分佈配置約 10 萬孕婦，挪威政府由 1999 年至 2008 年進行長達 10 年的長期追蹤，特別的是，所蒐集的資料還包括孕婦、配偶及嬰兒的生物醫學的資料(包括 DNA)，爲了有效運用這些資料，Norwegian Institute of Public Health 自 2006 年 9 月設置 Biobank 部門，正式對外提供，至 2008 年底已有 9 個申請案獲許可使用。

向 Norwegian Institute of Public Health 申請使用健康資料進行研究時，該機構除了負責審查並提供資料，還肩負研究資源協調的工作。也就是說，該機構對某些資料庫，如 Medical Birth of Registry，是採取儘量提供、鼓勵競爭，但對於某些資料庫，如 MoBa，則限定機構才能申請，同時希望不同計畫能彼此合作，不重複進行相同主題的研究，所以一旦同意提供，該機構會在未來 2~3 年間，不再允許相同主題的研

究進行，這種資料提供方式有時會遭到一些批評，但 Director Per Magnus 特別強調這個機制的重要性。所以審查通過的申請案必須與該機構簽訂資料使用合約。

2. NSD 擁有 Individual Level Data、Regional Data、Data on the Political System、Information on Research and Higher Education(DBH)四種不同類型的研究資料。其中的 Individual Level Data 目前約有 3000 多種資料集(Data Sets)，均可透過線上直接存取，這些資料集包括下列幾種：

(1)挪威國家統計局的普查資料庫(Census Data Bank)：不同於丹麥，挪威國家統計局自己並沒有對外服務，而是透過 NSD 提供資料；

(2)各研究專案所蒐集的個人資料：由挪威國家研究委員經費支持的研究需將資料存於 NSD，此外，因爲 Data Inspector Agency 不允許研究中所蒐集的資料，存放於研究者處，故多數研究者會將蒐集的資料放在 NSD；

(3)NSD 自己進行的調查研究資料：約 1500 種各式調查資料；

(4)其他資料庫：來自健康保險、社會福利或勞動市場的資料庫；

(5)跨國合作的統計調查資料：數千項歐洲社會調查、選舉或其他研究資料。

使用 NSD 的資料必須提出申請，每年約有 4000 件申請案件，由 Data Protection Official for Research 部門負責審查(成員共 14 人)。由於 Data Inspector Agency 將 NSD 視爲合作夥伴，資料使用申請不需先經過 Data Inspector Agency 許可，而由 NSD 審查後再向 Data Inspector Agency 報備。一般而言，NSD 站在協助的角色上，很少會否決申請，而是提供建議來幫助申請者取得最有用的研究資料，整個案件的審查視不同資料需求約需 1 週至 2 個月。大多數資料申請的服務是免費的，只有一些特殊服務才需要收費，例如特定資料的跨資料庫比對串接服務，這類服務還必需取的各資料庫的使用許可，且不能串接超過 10%資料。由於 NSD 能完善的服務及豐富的資料，大多數研究者喜歡與 NSD 合

作，NSD 也因此獲得更多的資料來源，形成良性循環，NSD 同時也是歐盟最重要的資料對外提供服務合作夥伴。

參、 心得與建議

此次赴北歐兩國考察，由於有特定之專業目的，因此係直接與該國之專責機構聯繫，從開始即得到友善回應，其後行程安排及接待縝密而慎重，參訪單位均派出相關業務主管簡報及與談，因此收穫良多。各參訪單位對我國健保制度及資料比對提供方式亦有高度興趣，紛紛要求參訪人介紹，提供地主單位可參考之經驗，例如 Danish Data Protection Agency 即表示要比照採用「全民健康保險研究資料庫」資料保密切結書。參訪心得及結論與建議分述如下：

一、 參訪心得

綜觀丹麥及挪威兩國的個人健康(保險)資料比對及對外提供，各有其特色。例如丹麥允許比對及提供可辨識個人的資料，挪威則已將蒐集的生物醫學個人資料提供研究使用。台灣的「全民健康保險研究資料庫」，資料內容豐富性及完整性與丹麥、挪威兩國相較，並不遜色，有些部分甚至有超越之處，例如初級照護資料即爲丹麥未及之處，而挪威資料庫雖多，卻不易收集完整的資料，其 NorPD 只含括約 70%的資料。目前丹麥及挪威的研究者藉由資料庫來進行許多具國際水準的研究，於國際期刊時有所聞，若能提升「全民健康保險研究資料庫」的功效，未來產生國際級研究是可以預期的。

透過實地參訪瞭解，丹麥及挪威兩國在個人資料比對及對外提供上，已有很好的法律規範及作業原則，然而，兩國人民良好的公民素養、研究者的自律精神也是維持制度運行不可或缺的條件。例如參訪丹麥 National Board of Health、Statistics Denmark 及 Data Protection Agency 時，各機構均表達對使用者深具信心，也不擔心網路駭客或資料外洩的問題，這是我們要參考這兩個國家的作法時，必須要注意到的客觀條件。藉由制度的設定及研究者的自律，才能使整個機制運作順利，不致產生重大缺失。

根據丹麥及挪威兩國的考察結果，台灣的「全民健康保險研究資料庫」在資料安全與保護個人隱私方面，是相當進步的，將個人識別資料兩階段加密，強化資料洩露時的追蹤管理機制。此外，資料比對串接後，對可能遭辨識資料進行模糊化處理的最小資料原則，與丹麥 National Board of Health 相同，均爲 20%。最後，在審查時間、資料銷毀機制及資訊公開上，均與先進國家作法相近，表示在本局與國衛院的共同努力下，「全民健康保險研究資料庫」的運作是值得肯定的。

二、 結論與建議

藉此次雙方之交流，除獲得先進國家寶貴與重要的第一手資訊外，也促進雙方友誼，爲後續合作及資訊交流建立了良好的溝通網絡。最後提出兩點建議供後續政策與執行規劃參考。

(一)訂定更完善的法律規範及作業原則

丹麥、挪威兩國自 2000 年起透過個人資料處理法案提供了明確的法律規範及作業原則，對使用資料庫從事研究工作的研究者來說，非常有利，良好的法規環境與建全的審查機制，可以讓資料在安全的情形下，更有效率的進行資料提供服務。我國雖已通過個人資料保護法，但對於醫療(健康)資料蒐集、處理或利用，尚未訂定相關辦法，故行政院研考會整理「總統政見執行追蹤一覽表」之「16.人權政策」提到的政府資料庫不得恣意聯結，也就缺乏明確法律規範及作業原則，期待主管機關能參考北歐兩國的相關法案，早日研訂醫療(健康)資料的處理法規。

(二) 資料提供建議朝網路、線上發展

透過網際網路線上存取資料已是趨勢，在雲端運算的發展概念下，資料服務只有透過網際網路才能進行更大規模的合作與發展，不只「全民健康保險研究資料庫」，包括行政院衛生署的「健康資料加值應用協作中心」均應及早規劃朝網路服務發展，研發相關管理技術。建議初期可採類似丹麥 Statbank 或挪威 Norhealth，提供整體性分析資料(Marco Data)，成熟後再提供明細資料(Micro Data)分析服務。

附錄一、參訪機構資料表

參訪機構	地址	主管代表	聯絡人
Danish National Board of Health	Islands Brygge 67 DK-2300 Copenhagen	Dorte Hansen Thrige, Head of Documentation Department	Monika Madsen, Assistant Manager
Statistics Denmark	Sejroegade 11, DK-2100 Copenhagen	Bo Johansen, Chief Adviser of Director General's Staff	Rasmus Jul Larsen, Head of International Consulting Division
Danish Data Protection Agency	Borgergade 28, DK-1300 Copenhagen	Camilla Daasness, Special Consultant	Maiken Breüner, Legal Consultant
Norwegian Institute of Public Health	Lovisenberggata 6 and 8, 0456 Oslo	Per Magnus, Director of the Division of Epidemiology	Berit Myklebust
Norwegian Social Science Data Services	Harald Hårfagres gate 29, N-5007 Bergen	Bjorn Henrichsen, Executive Director	Bjorn Henrichsen, Executive Director

附錄二、丹麥個人資料處理法案(節錄)

Act No. 429 of 31 May 2000 as amended by section 7 of Act No. 280 of 25 April 2001, section 6 of Act No. 552 of 24 June 2005, section 2 of Act No. 519 of 6 June 2007, section 1 of Act No. 188 of 18 March 2009 and section 2 of Act No. 503 of 12 June 2009
(This version is translated for the Danish Data Protection Agency. The official version is published in "Lovtidende" (Official Journal) on 2 June 2000. Only the Danish version of the text has legal validity.)

The Act on Processing of Personal Data

WE MARGRETHE THE SECOND, by the Grace of God, Queen of Denmark make known that: Folketinget (the Danish Parliament) has passed and we have granted Our Royal Assent to the following Act:

Title I General Provisions

Chapter 1 Scope of the Act

1. - (1) This Act shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

(2) This Act shall further apply to other non-automatic systematic processing of data which is performed for private persons or bodies and which includes data on individual persons' private or financial matters or other data on personal matters which can reasonably be claimed to be withheld from the public. However, this shall not apply to Chapters 8 and 9 of this Act.

(3) Section 5 (1) to (3), sections 6 to 8, section 10, section 11 (1), section 38 and section 40 of the Act also apply to manual transmission of personal data to another administrative authority. The Danish Data Protection Agency is responsible for the supervision of such transmission, in accordance with chapter 16 of the Act, as mentioned in the first sentence.

(4) This Act shall further apply to the processing of data concerning companies, etc., cf. subsections (1) and (2), if the processing is carried out for credit information agencies. The same shall apply in the case of processing of data covered by section 50 (1) 2.

(5) Chapter 5 of the Act shall also apply to the processing of data concerning companies, etc., cf. subsection (1).

(6) In other cases than those mentioned in subsection (3), the Minister of Justice may

decide that the provisions of this Act shall apply, in full or in part, to the processing of data concerning companies, etc. which is performed for private persons or bodies.

(7) In other cases than those mentioned in subsection(4), the competent Minister may decide that the provisions of this Act shall apply, in full or in part, to the processing of data concerning companies, etc., which is performed on behalf of public administrations.

(8) This Act shall apply to any processing of personal data in connection with video surveillance.

2. - (1) Any rules on the processing of personal data in other legislation which give the data subject a better legal protection shall take precedence over the rules laid down in this Act.

(2) This Act shall not apply where this will be in violation of the freedom of information and expression, cf. Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(3) This Act shall not apply to the processing of data undertaken by a natural person with a view to the exercise of purely personal activities.

(4) The provisions laid down in Chapters 8 and 9 and sections 35 to 37 and section 39 shall not apply to processing of data which is performed on behalf of the courts in the area of criminal law. Nor shall the provisions laid down in Chapter 8 of the Act and sections 35 to 37 and section 39 apply to processing of data which is performed on behalf of the police and the prosecution in the area of criminal law.

(5) This Act shall not apply to the processing of data which is performed on behalf of Folketinget (the Danish Parliament) and its related institutions.

(6) This Act shall not apply to the processing of data covered by the Act on information databases operated by the mass media.

(7) This Act shall not apply to information databases which exclusively include already published periodicals or sound and image programmes covered by paragraphs 1 or 2 of section 1 of the Act on media responsibility, or part hereof, provided that the data are stored in the database in the original version published. However, sections 41, 42 and 69 of the Act shall apply.

(8) Furthermore, this Act shall not apply to information databases which exclusively include already published texts, images and sound programmes which are covered by paragraph 3 of section 1 of the Act on media responsibility, or parts hereof, provided that the data are stored in the database in the original version published. However, sections 41, 42 and 69 of the Act shall apply.

(9) This Act shall not apply to manual files of cuttings from published, printed articles which are exclusively processed for journalistic purposes. However, sections 41, 42 and 69 of the Act shall apply.

(10) Processing of data which otherwise takes place exclusively for journalistic purposes shall be governed solely by sections 41, 42 and 69 of this Act. The same shall apply to the processing of data for the sole purpose of artistic or literary expression.

(11) This Act shall not apply to the processing of data which is performed on behalf of the intelligence services of the police and the national defense.

Chapter 2 Definitions

3. - (1) For the purpose of the Act:

1. 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject');

2. 'processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means;

3. 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

4. 'controller' shall mean 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 personal data;

5. 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

6. 'third party' shall mean any natural or legal person;

7. 'public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data; 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

8. 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

9. 'third country' shall mean any state which is not a member of the European Community and which has not implemented agreements entered into with the European Community which contain rules corresponding to those laid down in Directive 95/46/EC 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.

Chapter 3 Geographical territory of the Act

4.- (1) This Act shall apply to processing of data carried out on behalf of a controller who

is established in Denmark, if the activities are carried out within the territory of the European Community.

(2) This Act shall further apply to processing carried out on behalf of Danish diplomatic representations.

(3) This Act shall also apply to a controller who is established in a third country, if

1. the processing of data is carried out with the use of equipment situated in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the European Community; or
2. the collection of data in Denmark takes place for the purpose of processing in a third country.

(4) A controller who is governed by this Act by rule of paragraph 1 of subsection (3) must appoint a representative established in the territory of Denmark. This shall be without prejudice to legal actions which could be initiated by the data subject against the controller concerned.

(5) The controller shall inform the Data Protection Agency in writing of the name of the appointed representative, cf. subsection (4).

(6) This Act shall apply where data are processed in Denmark on behalf of a controller established in another Member State and the processing is not governed by Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of data and on the free movement of such data. This Act shall also apply if data are processed in Denmark on behalf of a controller established in a state which has entered into an agreement with the European Community which contains rules corresponding to those laid down in the above-mentioned Directive and the processing is not governed by these rules.

Title II Rules on processing of data

Chapter 4 Processing of data

5. - (1) Data must be processed in accordance with good practices for the processing of data.

(2) Data must be collected for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes. Further processing of data which takes place exclusively for historical, statistical or scientific purposes shall not be considered incompatible with the purposes for which the data were collected.

(3) Data which are to be processed must be adequate, relevant and not excessive in relation to the purposes for which the data are collected and the purposes for which they are subsequently processed.

(4) The processing of data must be organised in a way which ensures the required

up-dating of the data. Furthermore, necessary checks must be made to ensure that no inaccurate or misleading data are processed. Data which turn out to be inaccurate or misleading must be erased or rectified without delay.

(5) The data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed.

6. - (1) Personal data may be processed only if:

1. the data subject has given his explicit consent; or
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
3. processing is necessary for compliance with a legal obligation to which the controller is subject; or
4. processing is necessary in order to protect the vital interests of the data subject; or
5. processing is necessary for the performance of a task carried out in the public interest; or
6. processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
7. processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

(2) A company may not disclose data concerning a consumer to a third company for the purpose of marketing or use such data on behalf of a third company for this purpose, unless the consumer has given his explicit consent. The consent shall be obtained in accordance with the rules laid down in section 6 of the Danish Marketing Act.

(3) However, the disclosure and use of data as mentioned in subsection (2) may take place without consent in the case of general data on customers which form the basis for classification into customer categories, and if the conditions laid down in subsection (1) 7 are satisfied.

(4) Data of the type mentioned in sections 7 and 8 may not be disclosed or used by virtue of subsection (3). The Minister of Justice may lay down further restrictions in the access to disclose or use certain types of data by virtue of subsection (3).

7. - (1) No processing may take place of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life.

(2) The provision laid down in subsection (1) shall not apply where:

1. the data subject has given his explicit consent to the processing of such data; or
2. processing is necessary to protect the vital interests of the data subject or of another person where the person concerned is physically or legally incapable of giving his consent; or
3. the processing relates to data which have been made public by the data subject; or
4. the processing is necessary for the establishment, exercise or defence of legal claims.

(3) Processing of data concerning trade union membership may further take place where the processing is necessary for the controller's compliance with labour law obligations or specific rights.

(4) Processing may be carried out in the course of its legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or tradeunion aim of the data mentioned in subsection (1) relating to the members of the body or to persons who have regular contact with it in connection with its purposes. Disclosure of such data may only take place if the data subject has given his explicit consent or if the processing is covered by subsection (2) 2 to 4 or subsection (3).

(5) The provision laid down in subsection (1) shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy.

(6) Processing of the data mentioned in subsection (1) may take place where the processing is required for the performance by a public authority of its tasks in the area of criminal law.

(7) Exemptions may further be laid down from the provision in subsection (1) where the processing of data takes place for reasons of substantial public interests. The supervisory authority shall give its authorization in such cases. The processing may be made subject to specific conditions. The supervisory authority shall notify the Commission of any derogation.

(8) No automatic registers may be kept on behalf of a public administration containing data on political opinions which are not open to the public.

8. - (1) No data about criminal offences, serious social problems and other purely private matters than those mentioned in section 7 (1) may be processed on behalf of a public administration, unless such processing is necessary for the performance of the tasks of the administration.

(2) The data mentioned in subsection (1) may not be disclosed to any third party.

Disclosure may, however, take place where:

1. the data subject has given his explicit consent to such disclosure; or
2. disclosure takes place for the purpose of pursuing private or public interests which clearly override the interests of secrecy, including the interests of the person to whom the data relate; or
3. disclosure is necessary for the performance of the activities of an authority or required for a decision to be made by that authority; or
4. disclosure is necessary for the performance of tasks for an official authority by a person or a company.

(3) Administrative authorities performing tasks in the social field may only disclose the data mentioned in subsection (1) and the data mentioned in section 7 (1) if the conditions laid down in subsection (2) 1 or 2 are satisfied, or if the disclosure is a necessary step in the procedure of the case or necessary for the performance by an authority of its supervisory or control function.

(4) Private persons and bodies may process data about criminal offences, serious social problems and other purely private matters than those mentioned in section 7 (1) if the data subject has given his explicit consent. Processing may also take place if necessary for the purpose of pursuing a legitimate interest and this interest clearly overrides the interests of the data subject.

(5) The data mentioned in subsection (4) may not be disclosed without the explicit consent of the data subject. However, disclosure may take place without consent for the purpose of pursuing public or private interests, including the interests of the person concerned, which clearly override
the interests of secrecy.

(6) Processing of data in the cases which are regulated by subsections (1), (2), (4) and (5) may otherwise take place if the conditions laid down in section 7 are satisfied.

(7) A complete register of criminal convictions may be kept only under the control of a public authority.

9. - (1) Data as mentioned in section 7 (1) or section 8 may be processed where the processing is carried out for the sole purpose of operating legal information systems of significant public importance and the processing is necessary for operating such systems.

(2) The data covered by subsection (1) may not subsequently be processed for any other purpose. The same shall apply to the processing of other data which is carried out solely for the purpose of operating legal information systems, cf. section 6.

(3) The supervisory authority may lay down specific conditions concerning the processing operations mentioned in subsection (1). The same shall apply to the data mentioned in section 6 which are processed solely in connection with the operation of legal

information systems.

10. - (1) Data as mentioned in section 7 (1) or section 8 may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant public importance and where such processing is necessary in order to carry out these studies.

(2) The data covered by subsection (1) may not subsequently be processed for other than statistical or scientific purposes. The same shall apply to processing of other data carried out solely for statistical or scientific purposes, cf. section 6.

(3) The data covered by subsections (1) and (2) may only be disclosed to a third party with prior authorization from the supervisory authority. The supervisory authority may lay down specific conditions concerning the disclosure.

11. - ~ 14. - (略)

Chapter 5 Disclosure to credit information agencies of data on debts to public authorities

15. - ~ 26. - (略)

Chapter 6a Video surveillance

26 a. - ~ 26c. - (略)

Chapter 7 Transfer of personal data to third countries

27. - (略)

Title III The data subject' s rights

Chapter 8 Information to be given to the data subject

28. - (1) Where the personal data have been collected from the data subject, the controller or his representative shall provide the data subject with the following information:

1. the identity of the controller and of his representative;
2. the purposes of the processing for which the data are intended;
3. any further information which is necessary, having regard to the specific circumstances in which the personal data are collected, to enable the data subject to safeguard his interests, such as:

(a) the categories of recipients;

(b) whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply;

(c) the rules on the right of access to and the right to rectify the data relating to the

data subject.

(2) The provisions of subsection (1) shall not apply where the data subject already has the information mentioned in paragraphs 1 to 3.

29. - (1) Where the data have not been obtained from the data subject, the controller or his representative shall at the time of undertaking the registration of the data, or where disclosure to a third party is envisaged, no later than the time when the data are disclosed, provide the data subject with the following information:

1. the identity of the controller and of his representative;
2. the purposes of the processing for which the data are intended;
3. any further information which is necessary, having regard to the specific circumstances in which the data are obtained, to enable the data subject to safeguard his interests, such as:
   (a) the categories of data concerned;
   (b) the categories of recipients;
   (c) the rules on the right of access to and the right to rectify the data relating to the data subject.

(2) The rules laid down in subsection (1) shall not apply where the data subject already has the information referred to in paragraphs 1 to 3 or if recording or disclosure is expressly laid down by law or regulations.

(3) The rules laid down in subsection (1) shall not apply where the provision of such information to the data subject proves impossible or would involve a disproportionate effort.

30. - (1) Section 28 (1) and section 29 (1) shall not apply if the data subject' s interest in obtaining this information is found to be overridden by essential considerations of private interests, including the consideration for the data subject himself.

(2) Derogations from section 28 (1) and section 29 (1) may also take place if the data subject' s interest in obtaining this information is found to be overridden by essential considerations of public interests, including in particular:

1. national security;
2. defence;
3. public security;
4. the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions;
5. important economic or financial interests of a Member State or of the European Union, including monetary, budgetary and taxation matters; and
6. monitoring, inspection or regulatory functions, including temporary tasks,

connected with the exercise of official authority in cases referred to in paragraphs 3 to 5.

Chapter 9 The data subject’ s right of access to data

31. - ~ 34. - (略)

Chapter 10 Other rights

35. - ~ 40. - (略)

Title IV Security

Chapter 11 Security of processing

41. - (1) Individuals, companies etc. performing work for the controller or the processor and who have access to data may process these only on instructions from the controller unless otherwise provided by law or regulations.

(2) The instruction mentioned in subsection (1) may not restrict journalistic freedom or impede the production of an artistic or literary product.

(3) The controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in this Act. The same shall apply to processors.

(4) As regards data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions.

(5) The Minister of Justice may lay down more detailed rules concerning the security measures mentioned in subsection (3).

42. - (1) Where a controller leaves the processing of data to a processor, the controller shall make sure that the processor is in a position to implement the technical and organizational security measures mentioned in section 41 (3) to (5), and shall ensure compliance with those measures.

(2) The carrying out of processing by way of a processor must be governed by a written contract between the parties. This contract must stipulate that the processor shall act only on instructions from the controller and that the rules laid down in section 41 (3) to (5) shall also apply to processing by way of a processor. If the processor is established in a different Member State, the contract must stipulate that the provisions on security measures laid down by the law in the Member State in which the processor is established shall also be incumbent on the processor.

Title V Notification

Chapter 12 Notification of processing carried out for a public administration

43. - (1) The controller or his representative shall notify the Data Protection Agency before processing of data is carried out on behalf of the public administration, cf., however, section 44. The controller may authorize other authorities or private bodies to make such notifications on his behalf.

(2) The notification must include the following information:

1. the name and address of the controller and of his representative, if any, and of the processor, if any;
2. the category of processing and its purpose;
3. a general description of the processing;
4. a description of the categories of data subjects and of the categories of data relating to them;
5. the recipients or categories of recipients to whom the data may be disclosed;
6. intended transfers of data to third countries;
7. a general description of the measures taken to ensure security of processing;
8. the date of the commencement of the processing;
9. the date of erasure of the data.

44. - (1) Processing operations which do not cover data of a confidential nature shall be exempt from the rules laid down in section 43, cf., however, subsection (2). Such processing may further without notification include identification data, including identification numbers, and data concerning payments to and from public authorities, unless it is a matter of processing as mentioned in section 45 (1).

(2) The Minister of Justice shall lay down more detailed rules on the processing operations mentioned in subsection (1).

(3) Processing for the sole purpose of keeping a register which according to law or regulations is intended to provide information to the public in general and which is open to public consultation shall also be exempt from the rules laid down in section 43.

(4) The Minister of Justice may lay down rules to the effect that certain categories of processing of data shall be exempt from the provisions laid down in section 43. This shall, however, not apply to the categories of processing mentioned in section 45 (1).

45. - (1) Before processing operations covered by the obligation to notify in section 43 are carried out, the opinion of the Danish Data Protection Agency must be obtained where:

1. processing includes data which are covered by section 7 (1) and section 8 (1); or

2. processing is carried out for the sole purpose of operating legal information systems; or
3. processing is carried out solely for scientific or statistical purposes; or
4. processing includes alignment or combination of data for control purposes.

(2) The Minister of Justice may lay down rules to the effect that the opinion of the Agency shall be obtained prior to the start of any other processing operations than those mentioned in subsection (1).

46. - (1) Changes in the information mentioned in section 43 (2) shall be notified to the Agency prior to being implemented. Less important changes may be notified subsequently, at the latest 4 weeks after the implementation.

(2) The opinion of the Agency shall be obtained prior to the implementation of changes in the information mentioned in section 43 (2) contained in notifications of processing operations covered by section 45 (1) or (2). Less important changes shall only be notified. Notification may take place subsequently, at the latest 4 weeks after the implementation.

47. - (1) In cases where the data protection responsibility has been delegated to a subordinate authority and the Agency cannot approve the carrying out of a processing operation, the matter shall be brought before the competent Minister who shall decide the matter.

(2) If the Agency cannot approve the carrying out of a processing operation on behalf of a municipal or county authority, the matter shall be brought before the Minister of the Interior who shall decide the matter.

Chapter 13 Notification of processing operations carried out on behalf of a private controller

48. - (1) Prior to the commencement of any processing of data which is carried out on behalf of a private controller, the controller or his representative must notify the Danish Data Protection Agency, cf., however, section 49.

(2) The notification must include the information mentioned in section 43 (2).

49. - (1) Processing of data shall, except in the cases mentioned in section 50 (2), be exempt from the rules laid down in section 48 where:

1. the processing relates to data about employees, to the extent that the processing does not include data as mentioned in section 7 (1) and section 8 (4); or
2. the processing relates to data concerning the health of employees, to the extent that the pro-cessing of health data is necessary to comply with provisions laid down by

law or regulations; or

3. the processing relates to data concerning employees if registration is necessary under collective agreements or other agreements on the labour market; or
4. the processing relates to data concerning customers, suppliers or other business relations, to the extent that the processing does not include data as mentioned in section 7 (1) and section 8 (4), or to the extent that it is not a matter of processing operations as mentioned in section 50 (1) 4; or
5. the processing is carried out for the purpose of market surveys, to the extent that the processing does not include data as mentioned in section 7 (1) and section 8 (4); or
6. the processing is carried out by an association or similar body, to the extent that only data concerning the members of the association are processed; or
7. the processing is carried out by lawyers or accountants in the course of business, to the extent that only data concerning client matters are processed; or
8. the processing is carried out by doctors, nurses, dentists, dental technicians, chemists, therapists, chiropractors and other persons authorized to exercise professional activities in the health sector, to the extent that the data are used solely for these activities and the processing of the data is not carried out on behalf of a private hospital; or
9. the processing is carried out for the purpose of being used by an occupational health service.

(2) The Minister of Justice shall lay down more detailed rules concerning the processing operations mentioned in subsection (1).

(3) The Minister of Justice may lay down rules to the effect that other types of processing operations shall be exempt from the provision laid down in section 48. However, this shall not apply to processing operations covered by section 50 (1) unless the processing operations are exempted under section 50 (3).

50. - ~ 51. - (略)

Chapter 14 Notification of processing operations carried out on behalf of the courts

52. The rules laid down in sections 43 to 46 shall apply to the notification to the Danish Court Administration of processing of data carried out on behalf of the courts.

Chapter 15 Miscellaneous provisions

53. - ~ 54. - (略)

Title VI Supervision and final provisions

Chapter 16 The Data Protection Agency

55. - (1) The Data Protection Agency, which consists of a Council and a Secretariat, is responsible for the supervision of all processing operations covered by this Act, cf., however chapter 17.

(2) The day-to-day business is attended to by the Secretariat, headed by a Director.

(3) The Council, which shall be set up by the Minister of Justice, is composed of a chairman, who shall be a legally qualified judge, and of six other members. Substitutes may be appointed for the members of the Council. The members and their substitutes shall be appointed for a term of 4 years.

(4) The Council shall lay down its own rules of procedure and detailed rules on the division of work between the Council and the Secretariat.

56. The Data Protection Agency shall act with complete independence in executing the functions entrusted to it.

57. The opinion of the Data Protection Agency shall be obtained when Orders, Circulars or similar general regulations of importance for the protection of privacy in connection with the processing of data are to be drawn up.

58. - (1) The Data Protection Agency shall supervise, on its own initiative or acting on a complaint from a data subject, that the processing is carried out in compliance with the provisions of this Act and any rules issued by virtue of this Act.

(2) The Data Protection Agency may at any time revoke a decision made in accordance with section 27 (4) or section 50 (2), cf. section 27 (1) or (3) 2 to 4, if the European Commission decides that transfer of data to specific third countries may not take place or whether such transfers may lawfully take place. This, however, shall only apply where the revocation is necessary in order to comply with the decision of the Commission.

59. - (1) The Data Protection Agency may order a private data controller to discontinue a processing operation which may not take place under this Act and to rectify, erase or block specific data undergoing such processing.

(2) The Data Protection Agency may prohibit a private data controller from using a specified procedure in connection with the processing of data if the Data Protection Agency finds that the procedure in question involves a considerable risk that data are processed in violation of this Act.

(3) The Data Protection Agency may order a private data controller to implement specific technical and organizational security measures to protect data which may not be processed against processing, and to protect data against accidental or unlawful destruction

or accidental loss, alteration, and disclosure to any unauthorized person, abuse or any other unlawful forms of processing.

(4) The Data Protection Agency may in special cases issue a prohibitory or mandatory injunction against data processors, cf. subsections (1) to (3).

60. - (1) The Data Protection Agency shall make decisions in relation to the relevant authority in cases concerning section 7 (7), section 9 (3), section 10 (3), section 13 (1), section 27 (4), sections 28 to 31, section 32 (1), (2) and (4), sections 33 to 37, section 39 and section 58 (2).

(2) In other cases, the Data Protection Agency shall give opinions to the authority acting as controller.

61. No appeals may be brought before any other administrative authority against the decisions made by the Data Protection Agency under the provisions of this Act.

62. - (1) The Data Protection Agency may require to be furnished with any information of importance to its activities, including for the decision as to whether or not a particular matter falls under the provisions of this Act.

(2) The members and the staff of the Data Protection Agency shall at any time, against appropriate proof of identity and without any court order, have access to all premises from which processing operations carried out on behalf of the public administration are administered, or from which there is access to the data subject to processing, and to all premises where data or technical equipment are stored or used.

(3) Subsection (2) shall apply correspondingly as regards processing operations carried out on behalf of private data controllers to the extent that such processing is covered by section 50 or is carried out in connection with video surveillance.

(4) Subsection (2) shall also apply to processing operations carried out by processors as referred to in section 53.

63. - (1) The Data Protection Agency may decide that notifications and applications for authorizations under the provisions of this Act and any changes therein may or shall be submitted in a specified manner.

(2) An amount of DKK 1,000 shall be payable in connection with the submission of the following notifications and applications for authorizations under this Act:

1. Notifications under section 48.
2. Authorizations under section 50.
3. Notifications under section 53.

(3) Notifications as referred to in subsection (2) 1 and 3 shall be deemed to have been

submitted only when payment has been effected. The Data Protection Agency may decide that authorizations as referred to in subsection (2) 2 shall not be granted until payment has been effected.

(4) The provisions of subsection (2) 1 and 2 do not apply to processing of data which takes place exclusively for scientific or statistical purposes.

(5) Where a processing operation shall both be notified under section 48 and authorized under section 50, only a single fee shall be payable.

64. - (1) The Data Protection Agency may, on its own initiative or at the request of another Member State, check that a processing operation of data taking place in Denmark is lawful, irrespective of whether or not the processing operation is governed by the legislation of another Member State. The provisions laid down in sections 59 and 62 shall be correspondingly applicable.

(2) The Data Protection Agency may further disclose data to supervisory authorities in other Member States to the extent that this is required in order to ensure compliance with the provisions of this Act or those of the data protection legislation of the Member State concerned.

65. The Data Protection Agency shall submit an annual report on its activities to Folketinget (the Danish Parliament). The report shall be made public. The Data Protection Agency may also make its opinions accessible to the general public. Section 30 shall be correspondingly applicable.

66. The Data Protection Agency and the Danish Court Administration shall co-operate to the extent required to fulfil their obligations, particularly through the exchange of all relevant data.

Chapter 17 Supervision of the courts

67. - ~ 68. - (略)

Chapter 18 Liability in damages and criminal liability

69. - ~ 71. - (略)

Chapter 19 Final provisions, including commencement provisions, etc.

72. - ~ 83. - (略)

附錄三、挪威個人健康資料建檔法

Act of 18 May 2001 No. 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act)

Chapter 1 Purpose, definitions, substantive scope and extent of the Act

Section 1 Purpose of the Act

The purpose of this Act is to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy, so as to ensure that medical assistance may be provided in an adequate, effective manner. Through research and statistics, the Act shall contribute towards information on and knowledge of the state of public health, causes of impaired health and illness trends for administration, quality assurance, planning and management purposes. The Act shall ensure that personal health data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and respect for private life and ensure that personal health data are of adequate quality.

Section 2 Definitions

For the purposes of this Act, the following definitions shall apply:

1. personal health data: any information subject to the duty of confidentiality pursuant to the Health Personell Act section 21 and other information and assessments regarding health matters or that are significant for health matters, that may be linked to a natural person,

2. de-identified personal health data: personal health data from which the name, personal identity number and other characteristics serving to identify a person have been removed, so that the data can no longer be linked to a natural person, and where the identity can only be traced through alignment with the same data that were previously removed,

3. anonymous data: data from which the name, personal identity number and other characteristics serving to identify a person have been removed, so that the data can no longer be linked to a natural person,

4. pseudonymous health data: personal health data in which the identity has been encrypted or otherwise concealed, but nonetheless individualized so that it is possible to follow each person through the health system without his identity being revealed,

5. processing of personal health data: any use of personal health data for a specific purpose, such as collection, recording, alignment, storage and disclosure or a combination of such uses,

6. personal health data filing systems: filing systems, records, etc. where personal health data are systematically stored so that information concerning a natur person may be retrieved,

7. health data filing system established for therapeutic purposes: a system of patient records and information or other personal health data filing system for the purpose of providing a basis for acts that have preventive, diagnostic, therapeutic, health-preserving or rehabilitative objective in relation to the individual patient and that are performed by health personnel, and the administration of such acts,

8. data controller: the person who determines the purpose of the processing of personal health data and which means are to be used, unless responsibility for such data control is specially prescribed in the Act or in regulations laid down pursuant to the Act,

9. data processor: the person who processes personal health data on behalf of the controller,

10. the data subject: the person to whom personal health data may be linked,

11. consent: any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal health data relating to him or her.

Section 3 Substantive scope of the Act

This Act shall apply to

1. processing of personal health data in the public health administration and public health services that takes place wholly or partly by automatic means to achieve the purposes set out in section 1, and

2. other processing of personal health data in the public health administration and public health services for such purposes, when the personal health data are part of or are intended to be part of a personal health data filing system.

This Act shall apply to both public and private activities.

The King in Council may by regulations decide that this Act or parts of this Act shall apply to the processing of personal health data outside the public health administration and public health services in order to fulfil the purposes set out in section 1.

The Act shall not apply to the processing of personal health data that is regulated by the Health Research Act.

Amended by Act of 15 June 2001 no. 93 (effective 1 Jan 2002 by Royal Decree of 14 Dec 2001 no. 1417), and of 20 June 2008 no. 44 (effective 1 July 2009 by Royal Decree of 26 June 2009 no. 865).

Section 4 Territorial extent of the Act

This Act shall apply to data controllers who are established in Norway. The King may by regulations decide that the Act shall wholly or partly apply to Svalbard and Jan Mayen,

and lay down special rules regarding the processing of personal health data for these areas. This Act shall also apply to data controllers who are established in states outside the territory of the EEA if the controller makes use of technical equipment in Norway. However, this shall not apply if such equipment is used only to transfer personal health data through Norway.
Controllers such as are mentioned in the second paragraph shall have a representative who is established in Norway. The provisions that apply to the controller shall also apply to the representative.

Chapter 2. Permission to process personal health data, establishment of personal health data filing systems, collection of data, etc.

Section 5 Processing of personal health data, obligation to obtain a licence, etc.

Personal health data may only be processed by automatic means when this is permitted pursuant to the Personal Data Act, sections 9 and 33, the Health Research Act, or it is so provided by statute and is not prohibited on other special legal grounds. The same applies to other processing of personal health data, if the data are part of, or are intended to be part of, a health data filing system.
The obligation to obtain a licence pursuant to section 33 of the Personal Data Act shall not apply to the processing of personal health data that takes place pursuant to regulations laid down pursuant to sections 6 to 8. Before personal health data may be obtained for processing pursuant to the first paragraph, the data subject must give his consent, unless otherwise provided by or pursuant to statute.
Sections 4-3 to 4-8 of the Patients' Rights Act shall apply correspondingly to consent pursuant to this Act. Children between 12 and 16 years of age may themselves make decisions regarding consent if, for reasons that should be respected, the patient does not wish the data to be made known to his parents or other persons with parental responsibility.
Amended by Act of 20 June 2008 no. 44 (effective 1 July 2009 by Royal Decree of 26 June 2009 no. 865).

Section 6 Personal health data filing system established for therapeutic purposes

Personal health data filing systems established for therapeutic purposes may be kept by automatic means. It shall be evident from the filing system who has recorded the data. This may be done by means of an electronic signature or corresponding secure documentation.
Regional health enterprises and health enterprises, municipalities and other public or private establishments which make use of personal health data filing systems established for therapeutic purposes shall be data controllers. The enterprise and the municipality may delegate responsibility for controlling the data.

The King may by regulations prescribe further rules regarding the processing of personal health data in personal health data filing systems established for therapeutic purposes, including rules regarding the approval of software and other matters as mentioned in section 16, fourth paragraph.

Amended by Act of 15 June 2001 no. 93 (effective 1 Jan 2002 by Royal Decree of 14 Dec 2001 no. 1417).

Section 6a Inter-institutional personal health data filing systems established for therapeutic purposes

Inter-institutional personal health data filing systems established for therapeutic purposes may only be established when this is so provided by this Act or other statute.

Inter-institutional personal health data filing systems established for therapeutic purposes may only contain specifically defined health data of limited scope as are necessary and relevant for inter-institutional cooperation for sound health assistance to patients. Such systems may only be established in addition to the personal health data filing systems established for therapeutic purposes that the institution establishes internally, confer section 3-2 of the Specialized Health Services Act of 2 July 1999 no. 61, and section 1-3.a of the Municipal Health Services Act of 19 November 1982 no. 66, confer sections 39 and 40 of the Health Care Personnel Act. Inter-institutional personal health data filing systems established for therapeutic purposes shall be kept by automatic means (electronically).

The King in Council may by regulations prescribe further rules regarding the establishment, operation and processing of personal health data in inter-institutional personal health data filing systems established for therapeutic purposes. Inter-institutional personal health data filing systems established for therapeutic purposes may only be established without the consent of the patient (Data Subject) insofar as this is necessary to achieve the purpose of the register. This provision does not permit the establishment of centralized personal health data filing systems for therapeutic purposes.

The regulations pursuant to the third paragraph shall state the purpose of the processing of the personal health data and which data shall be processed. Moreover, the regulations shall state who shall have the Data Controller responsibility for the data, including location, access, and access control; and give the patient (Data Subject) the right to object to the processing of personal health data in the register, or require consent to be obtained from the patient.

Added by Act of 19 June 2009 no. 68.

Section 6b Inter-institutional personal health data filing systems established for therapeutic purposes – health care personnel in a formal collaboration

The King in Council may by regulations prescribe rules regarding the establishment of inter-institutional personal health data filing systems for therapeutic purposes for the use of

health care personnel in a formal collaboration.

The regulations pursuant to the first paragraph shall identify the location of the Data Controller and prescribe rules for access and access control. The Data Controller shall ensure that the Patient Records and data filing systems in the formal collaboration are sound.

Where such systems are established, the inter-institutional personal health data filing system for therapeutic purposes shall be kept automatically (electronically) and shall replace the corresponding internal registers within the institutions. The duty to keep Patient Records as defined in sections 39 and 40 of the Health Care Personnel Act shall apply correspondingly.

Added by Act of 19 June 2009 no. 68.

Section 6c Personal health data filing systems for administration and case review

The King in Council may by regulations prescribe rules regarding the establishment of personal health data filing systems and processing of personal health data for the following purposes:

1. case review to determine if a free card or refund of private contribution will be granted, cf. section 2-6 of the Patients' Rights Act, section 5-5 of the Specialized Health Services Act, and Chapter 5 of the National Insurance Act.
2. administration and coordination of transport to attend for examination or treatment in the municipal and specialized health services, cf. section 2-1a of the Specialized Health Services Act, first paragraph, no. 6.

The regulations pursuant to the first paragraph shall state what data may be processed in the register and prescribe rules regarding the Data Controller for the data, including location of responsibility. The regulations may contain provisions regarding access to data, access control, etc.

The personal health data may be processed without the consent of the Data Subject. This does not include data relating to diagnosis or disease. The Data Subject may object to the automatic registration of information concerning payment of private contribution in a register established pursuant to the first paragraph, no. 1, and to the disclosure of information concerning whether the Data Subject must pay a private contribution.

Added by Act of 18 December 2009 no. 137 (effective 1 Jan 2010 by Royal Decree of 18 Dec 2009 no. 1583).

Section 7 Regional and local personal health data filing systems

No regional or local personal health data filing systems may be established other than those authorized by this Act or another statute.

The King in Council may by regulations issue further rules regarding the establishment of local personal health data filing systems and the processing of personal health data in local health data filing systems in order to perform functions pursuant to the Municipal Health Services Act, the Social Services Act, and the Communicable Diseases Act. The name, personal identity number or other characteristics that directly identify a natural person may only be processed with the consent of the data subject. The latter' s consent is not necessary if the regulations provide that the personal health data may only be processed in pseudonymized or de-identified form. The regulations shall state the purpose of the processing of the personal health data, which data may be processed, and, if appropriate, prescribe further rules as to who shall effect the pseudonymization and principles for how this shall be done. The regional health enterprise is the data controller, unless otherwise provided by the regulations. Responsibility for controlling the data may be delegated.
The King in Council may by regulations prescribe further rules regarding the establishment of local personal health data filing systems and the processing of personal health data in such filing systems in order to perform functions pursuant to the Municipal Health Services Act and the Communicable Diseases Control Act. The name, personal identity number or other characteristics that directly identify a natural person may only be processed with the consent of the data subject. The latter' s consent is not necessary if the regulations provide that the personal health data may only be processed in pseudonymized or de-identified form. The regulations shall state the purpose of the processing of the personal health data, which data may be processed, and if, appropriate, prescribe further rules as to who shall effect the pseudonymization and principles for how this shall be done. The municipality is the data controller, unless otherwise provided by the regulations. Responsibility for controlling the data may be delegated.
Amended by Act of 15 June 2001 no. 93 (effective 1 Jan 2002 by Royal Decree of 14 Dec 2001 no. 1417), and Act of 10 June 2005 no. 47.

Section 8 Central personal health data filing systems

No central filing systems for personal health data may be established other than those authorized by this Act or another statute.

The King in Council may by regulations prescribe further rules regarding the establishment of central personal health data filing systems and the processing of personal health data in central personal health data filing systems in order to perform functions pursuant to the Pharmacies Act, the Municipal Health Services Act, the Social Services Act, the Dental Health Services Act, the Communicable Diseases Act and the Specialized Health Services Act, including the general management and planning of services, quality improvement, research and statistics. The name, national identity number or other characteristics that directly identify a natural person may only be processed with the consent of the Data Subject. The latter' s consent is not necessary if the regulations

provide that the personal health data may only be processed in pseudonymized or anonymized form. If appropriate, the regulations shall prescribe further rules regarding who shall effect the pseudonymization and principles for how this shall be done.

In the following registers, the name, national identity number and other characteristics that directly identify a natural person may be processed without the consent of the Data Subject insofar as this is necessary to achieve the purpose of the register, and characteristics that directly identify a natural person shall be stored in encrypted form in the register:

1. Causes of Death Registry
2. Cancer Registry
3. Medical Birth Registry
4. System of notification of infectious diseases
5. The Central Tuberculosis Register
6. System for Vaccination Control (SYSVAK)
7. Defence Forces Health Records
8. Norwegian Register of Patient Records
9. National Database for Electronic Prescriptions
10. National Register of Cardiovascular Disease

The requirement that characteristics that directly identify a natural person shall be stored in encrypted form in the register shall not apply to the National Database for Electronic Prescriptions.

The King in Council may by regulations issue further rules regarding the processing of the personal health data in the personal health data filing systems.

The regulations pursuant to the second and fourth paragraphs shall state the purpose of the processing of the personal health data and which data shall be processed. Moreover, the regulations shall state who shall be the Data Controller responsible for the data.

Responsibility for controlling the data may be delegated. The regulations should also prescribe rules regarding the duty of the Data Controller to make data available so that the purposes may be achieved.

Amended by Act of 2 July 2004 no. 59 (effective 1 Jan 2005 by Royal Decree 10 Dec 2004 no. 1614), Act of 10 June 2005 no. 47, Act of 16 Feb 2007 no. 7, Act of 15 June 2007 no. 32, and Act of 9 April 2010 no. 14.

Section 9 Particularly concerning the collection of personal health data for central, regional and local personal health data filing systems, the duty to report, etc.

Establishments and health care personnel who offer or provide services in accordance with the Pharmacies Act, the Municipal Health Services Act, the Social Services Act, the

Communicable Diseases Act, the Specialized Health Services Act or the Dental Health Services Act have a duty to disclose or transfer data as prescribed in regulations pursuant to sections 6c, 7 and 8 and pursuant to this section.

The King in Council may issue regulations regarding the collection of personal health data pursuant to sections 6c, 7 and 8, including rules regarding who shall give and receive data and regarding time limits, requirements as regards the form in which the data is to be provided and reporting forms. The recipient of the data shall notify the person sending the data if the data are deficient.

Amended by Act of 10 June 2005 no. 47, Act of 19 June 2009 no. 68, Act of 18 Dec 2009 no. 137 (effective 1 Jan 2010 by Royal Decree of 18 Dec 2009 no. 1583).

Section 10 Particularly concerning the duty to report data for statistical purposes

The Ministry may by regulations or by administrative decision order regional health enterprises and health enterprises, counties and municipalities to report de-identified or anonymous data for statistical purposes, including issuing further rules regarding the use of standards, classification systems and coding systems.

Amended by Act of 15 June 2001 no. 93 (effective 1 Jan 2002 by Royal Decree of 14 Dec 2001 no. 1417).

Chapter 3 General rules regarding the processing of personal health data

Section 11 Requirements regarding specification of purpose, objectiveness, relevance, etc.

All processing of personal health data shall have an explicitly stated purpose that is objectively justified by the activities of the data controller. The controller shall ensure that the personal health data that are processed are relevant to and necessary for the purpose of the processing of the data.

Personal health data may only be used for purposes other than the provision of medical assistance for the individual patient or for the administration of such assistance when it is necessary for the person to be identifiable in order to achieve these purposes. Reasons shall always be given for why it is necessary to use data relating to an identifiable person. Pursuant to section 31, the supervisory authority may require that the data controller present the reasons.

Personal health data may not be used for purposes that are incompatible with the original purpose of the collection of the data without the consent of the data subject.

Section 12 Alignment of personal health data

Personal health data in personal health data filing systems established for therapeutic purposes may be aligned with data relating to the same patient in another personal health data filing system established for therapeutic purposes to the extent that the personal health

data may be disclosed pursuant to sections 25, 26 and 45 of the Health Care Personnel Act.

Personal health data that is processed in personal health data filing systems as mentioned in section 6c may be mutually aligned in accordance with the purposes of the personal health data filing systems.

Personal health data collected pursuant to section 9 may be aligned in accordance with further rules prescribed in regulations laid down pursuant to sections 7 and 8.

Personal health data that is processed according to the first, second and third paragraphs may be aligned with data from the National Population Register relating to the Data Subject.

Beyond what is authorized by this section, personal health data may only be aligned when this is authorized pursuant to sections 9 and 33 of the Personal Data Act.

Amended by Act of 18 Dec 2009 no. 137 (effective 1 Jan 2010 by Royal Decree of 18 Dec 2009 no. 1583).

Section 13 Access to personal health data in the data controller's and the data processor's institution

Only the data controller, the data processors and persons working under the instructions of the controller or the processor may be granted access to personal health data. Access may only be granted insofar as this is necessary for the work of the person concerned and in accordance with the rules that apply regarding the duty of confidentiality.

The King in Council may by regulations issue further rules regarding the access to personal health data. For purposes of access to personal health data in personal health data filing systems established for therapeutic purposes the regulations may exempt from the first paragraph, first sentence.

Access to personal health data in personal health data filing systems established for therapeutic purposes may only be given following express consent from the Data Subject.

The King in Council may by regulations exempt from the requirement for express consent in the third paragraph, confer section 2, no. 11.

A request for personal health data and access to personal health data from another enterprise may only include one patient at a time.

The Data Subject shall have the right to view the log of the personal health data filing system established for therapeutic purposes that indicates who has had access to the personal health data regarding his/her person.

Amended by Act of 19 June 2009 no. 68.

Section 13a Prohibition of unlawful access to personal health data

It is forbidden to read, search or in other manner acquire, use or possess personal health data that is processed pursuant to this Act except when justified for reasons of providing

health assistance to the patient, administration of such health assistance, or as specifically authorized in statute or regulation.

Added by Act of 9 May 2008 no. 34 (effective 9 May 2008 by Royal Decree of 9 May 2008 no. 442).

Section 14 Disclosure of personal health data

Personal health data may be disclosed or transferred for alignment that is authorized pursuant to section 12. Aligned personal health data may, after the name and personal identity number have been removed, be disclosed or transferred to an enterprise as decided by the Ministry, when the purpose is to de-identify or anonymize the data.

Personal health data may, moreover, be disclosed or transferred when disclosure or transfer is authorized by or pursuant to statute, and the recipient of the data is authorized to process them pursuant to the Personal Data Act.

Section 15 Duty of secrecy

Any person who processes personal health data pursuant to this Act has a duty of secrecy pursuant to sections 13 to 13e of the Public Administration Act and the Health Care Personnel Act.

The duty of secrecy pursuant to the first paragraph also applies to the patient's place of birth, date of birth, personal identity number, pseudonym, nationality, civil status, occupation, residence and place of work.

Data may only be given to other administrative agencies pursuant to section 13b, nos. 5 and 6, of the Public Administration Act when this is necessary to facilitate the fulfilment of tasks pursuant to this Act, or to prevent significant danger to life or serious injury to a person's health.

The duty of secrecy shall nonetheless not prevent the disclosure of data to determine whether a patient must pay a private contribution to health care personnel or others who provide health assistance to the patient or provide other services to the patient which the National Insurance may be required to reimburse. Nor shall the duty of secrecy prevent the disclosure of such data to health institutions in connection with payment for patient transport.

Information about a patient's name, transport requirements and private contribution status, including the amount where applicable, may be disclosed to the transport provider in connection with transport covered by section 2-1a, first paragraph, no. 6 of the Specialized Health Services Act.

Amended by Act of 18 December 2009 no. 137 (effective 1 Jan 2010 by Royal Decree of 18 December 2009 no. 1583).

Section 15a Data relating to quality assurance, administration, planning or management of

a health service

Section 29b of the Health Care Personnel Act shall apply correspondingly to the processing of personal health data under this Act.

Added by Act of 9 April 2010 no. 14.

Section 16 Ensuring confidentiality, integrity, quality and accessibility

The data controller and the data processor shall by means of planned, systematic measures, ensure satisfactory data security with regard to confidentiality, integrity, quality and accessibility in connection with the processing of personal health data.

To achieve satisfactory data security, the controller and the processor shall document the data system and the security measures. Such documentation shall be accessible to the employees of the controller and of the processor. The documentation shall also be accessible to the supervisory authorities.

Any controller who allows other persons to have access to personal health data, e.g. a data processor or other persons performing tasks in connection with the data system, shall ensure that the said persons fulfil the requirements set out in the first and second paragraphs.

The King may prescribe regulations regarding data security in connection with the processing of personal health data pursuant to this Act. The King may for instance set further requirements as regards electronic signatures, communication and long-term storage, the authorization of software and the use of standards, classification systems and coding systems, and which national or international system of standards shall be followed.

Section 17 Internal control

The data controller shall establish and maintain such planned and systematic measures as are necessary to fulfil the requirements laid down in or pursuant to this Act, including measures to ensure the quality of personal health data.

The controller shall document the measures. The documentation shall be accessible to the employees of the controller and of the processor. The documentation shall also be accessible to the supervisory authorities.

The King may by regulations prescribe further rules regarding internal control.

Section 18 The data processor's right of disposition over personal health data

No data processor may process personal health data in any way other than that which is agreed in writing with the data controller. Nor may the data be handed over to another person for storage or manipulation without such agreement. It shall also be stated in the agreement with the controller that the processor undertakes to carry out such security measures as ensue from section 16.

Section 19 Time limit for replying to inquiries, etc.

The data controller shall reply to inquiries regarding access or other rights pursuant to sections 21, 22, 26 and 28 without undue delay and not later than 30 days from the date of receipt of the inquiry.

If special circumstances should make it impossible to reply to the inquiry within 30 days, implementation may be postponed until it is possible to reply. In such case, the controller shall give a provisional reply stating the reason for the delay and when a reply is likely to be given.

Chapter 4 The data controller's duty to provide information and the data subject's right to access

Section 20 Information to the general public regarding the processing of personal health data pursuant to sections 7 and 8 of this Act

When personal health data are processed in accordance with regulations laid down pursuant to sections 7 and 8, the controller shall on his own initiative inform the general public about what kind of processing of personal health data is being carried out.

Section 21 Right to general information on personal health data filing systems and processing of personal health data

Any person who so requests shall be informed of the kind of processing of personal health data a data controller is performing, and may demand to receive the following information as regards a specific type of processing:

1. the name and address of the controller and of his representative, if any,
2. who has the day-to-day responsibility for fulfilling the obligations of the controller,
3. the purpose of the processing of the personal health data,
4. descriptions of the categories of personal health data that are processed,
5. the sources of the data, and
6. whether the personal health data will be disclosed, and if so, the identity of the recipient.

The information may be demanded from the controller or from his processor as mentioned in section 18.

Section 22 Right of access

Any person who so requests has a right of access to personal health data filing systems established for therapeutic purposes insofar as this is authorized by section 5-1 of the Patients' Rights Act and section 41 of the Health Personnel Act.

When personal health data are processed pursuant to sections 5, 6c, 7 and 8, the Data Subject has the right, upon inquiry, in addition to the information specified in section 21, first paragraph, to be informed of:

1. the personal health data concerning the Data Subject that are being processed, and
2. the security measures implemented in connection with the processing of personal health data insofar as this knowledge does not prejudice security.

The data subject may also demand that the data controller elaborate on the information in section 21, first paragraph, to the extent that this is necessary to enable the data subject to protect his or her own interests.

Information pursuant to the first and second paragraphs may be demanded in writing from the controller or from his processor as mentioned in section 18. The person who is requested to grant access may demand that the data subject submit a written, signed request.

The King may by regulations issue further rules regarding the right of access to the processing of personal health data pursuant to the second and third paragraphs. If special reasons make this necessary, the King may issue regulations to the effect that the data subject must pay compensation to the controller. The compensation may not exceed the actual costs of complying with the demand.

Amended by Act of 18 December 2009 no. 137 (effective 1 Jan 2010 by Royal Decree of 18 Dec 2009 no. 1583).

Section 23 Obligation to provide information when data is collected from the data subject

When personal health data is collected from the data subject himself, the data controller shall on his own initiative first inform the data subject of

1. the name and address of the data controller and of his representative, if any,
2. the purpose of the processing of the personal health data,
3. whether the data will be disclosed and if, so, the identity of the recipient,
4. the fact that the provision of data is voluntary, and
5. any other circumstances that will enable the data subject to exercise his rights pursuant to this Act in the best possible way, such as information on the right to demand access to data, cf. section 22, and the right to demand that data be rectified and erased, cf. sections 26 and 28.

Notification is not required if there is no doubt that the data subject already has the information in the first paragraph.

Section 24 Obligation to provide information when data is collected from persons other than the data subject

A data controller who collects personal health data from persons other than the data subject

shall on his own initiative inform the data subject of the data which are being collected and provide such information as is mentioned in section 23, first paragraph, as soon as the data have been obtained. If the purpose of collecting the data is to communicate them to other persons, the controller may wait to notify the data subject until such disclosure takes place.
The data subject is not entitled to notification pursuant to the first paragraph if

1. the collection or communication of data is expressly authorized by statute,
2. notification is impossible or disproportionately difficult, or
3. there is no doubt that the data subject already has the information which shall be contained in the notification.

When notification is omitted pursuant to the second paragraph, no. 2, the information shall nonetheless be provided at the latest when the data subject is contacted on the basis of the data.

Section 25 Exceptions to the right to information and access

Access to personal health data filing systems established for therapeutic purposes may be denied pursuant to the provisions of section 5-1 of the Patients' Rights Act.
The right to access pursuant to sections 21 and 22, second paragraph, and the obligation to provide information pursuant to sections 20, 23 and 24 do not encompass data

1. which, if known, might endanger national security, national defence or the relationship to foreign powers or international organizations,
2. regarding which secrecy is required in the interests of the prevention, investigation, exposure and prosecution of criminal acts,
3. which it must be regarded as inadvisable for the data subject to gain knowledge of, out of consideration for the health of the person concerned or for the relationship to persons close to the person concerned,
4. to which a statutory obligation of professional secrecy applies,
5. which are solely to be found in texts drawn up for internal preparatory purposes and which have not been disclosed to other persons,
6. regarding which it will be contrary to obvious and fundamental private or public interests to provide information, including the interests of the data subject himself.

A representative of the patient is entitled to access to information to which the data subject is denied access pursuant to the first paragraph and second paragraph, no. 3, unless the representative is considered unfit thereto. A medical practitioner or lawyer may not be denied access, unless special grounds so indicate.
Any person who refuses to provide access to data pursuant to the first or second paragraph must give the reason for this in writing with a precise reference to the provision governing exceptions.

Chapter 5 Special rules regarding rectification and erasure of personal health data

Section 26 Rectification of deficient personal health data

If personal health data which are inaccurate, incomplete or of which processing is not authorized are processed pursuant to sections 5, 7 and 8, the data controller shall on his own initiative or at the request of the data subject rectify the deficient data. The controller shall if possible ensure that the error does not have an effect on the data subject. If the personal health data have been disclosed, the controller shall notify recipients of disclosed data.

The rectification of inaccurate or incomplete personal health data which may be of significance as documentation shall be effected by marking the data clearly and supplementing them with accurate data.

If weighty considerations relating to protection of privacy so warrant, the Data Inspectorate may, notwithstanding the second paragraph, decide that rectification shall be effected by erasing or blocking the deficient personal health data. If the data may not be destroyed pursuant to the Archives Act, the Director General of the National Archives of Norway shall be consulted prior to making an administrative decision regarding erasure. This decision shall take precedence over the provisions of sections 9 and 18 of the Archives Act of 4 December 1992 No. 126.

Erasure should be supplemented by the recording of accurate and complete data. If this is impossible, and the document that contained the erased data therefore provides a clearly misleading picture, the entire document shall be erased.

Sections 42 to 44 of the Health Personnel Act shall apply to rectification and erasure of personal health data in personal health data filing systems established for therapeutic purposes. The second and third sentences of the first paragraph apply correspondingly.

Section 27 Prohibition against storing unnecessary personal health data

The data controller shall not store personal health data longer than is necessary to carry out the purpose of the processing of the data. If the personal health data shall not thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased.

In regulations laid down pursuant to sections 6 to 8, it may be decided that personal health data may be stored for historical, statistical or scientific purposes, if the public interest in the data being stored clearly exceeds the disadvantages this may entail for the person concerned. In this case, the controller shall ensure that the data are not stored longer than necessary in ways that make it possible to identify the data subject.

Section 28 Erasure or blocking of personal health data which are regarded as disadvantageous by the data subject

The data subject may demand that personal health data processed pursuant to sections 5, 7 and 8 shall be erased or blocked if the processing is considered to be strongly disadvantageous to the data subject and there are no strong general considerations that warrant processing the data. The demand for the erasure or blocking of such data shall be made to the data controller.
After the Director General of the National Archives of Norway has been consulted, the Data Inspectorate may decide that the right to erase data pursuant to the first paragraph shall take precedence over the provisions of sections 9 and 18 of the Archives Act of 4 December 1992 No. 126. If the document that contained the erased data gives a clearly misleading picture after the erasure, the entire document shall be erased.
Demands for erasure of personal health data in personal health data filing systems established for therapeutic purposes shall be decided pursuant to section 43 of the Health Personnel Act.

Chapter 6 Supervision, control and sanctions

Section 29 Obligation to notify the Data Inspectorate

The data controller shall notify the Data Inspectorate before processing personal health data by automatic means and before establishing a manual personal health data filing system.
Notification shall be given not later than 30 days prior to commencement of the data processing. The Data Inspectorate shall give the controller a receipt of notification. New notification must be given prior to processing of personal health data that exceeds the limits for processing provided for in section 30. Even if no changes have taken place, new notification shall be given three years after the previous notification was given.
The King may prescribe regulations to the effect that certain methods of personal health data processing or data controllers are exempted from the obligation to give notification or are subject to a simplified obligation to give notification.

Section 30 Content of the notification

The notification to the Data Inspectorate shall provide information regarding

1. the name and address of the data controller and of his representative, if any, and the data processor,
2. when the processing of the personal health data will begin,
3. who has the day-to-day responsibility for fulfilling the obligations of the controller,
4. the purpose of the processing of the personal health data,
5. an overview of the categories of personal health data that are to be processed,
6. the sources of the personal health data,

7. the legal basis for collecting the personal health data,

8. the persons to whom the personal health data will be disclosed, including recipients in other countries, if any, and

9. the security measures related to the processing of the personal health data.

The King may prescribe regulations regarding the data that notifications shall contain and implementation of the obligation to give notification.

Section 31 The supervisory authorities

The Data Inspectorate exercises supervisory control that the provisions of the Act are complied with and that errors or deficiencies are rectified, cf. section 42 of the Personal Data Act, unless responsibility for supervision lies with the Norwegian Board of Health or the Chief County Medical Officer pursuant to the Act of 30 March 1984 no. 15 on government supervision of public health services.

The supervisory authorities may demand any data necessary to enable them to carry out their functions.

In connection with its verification of compliance with statutory provisions, the supervisory authorities may demand admittance to places where personal health data filing systems, personal health data that are processed automatically and technical aids for such processing are located. The supervisory authorities may carry out such tests or inspections as they deem necessary and may demand such assistance from the personnel in such places as is necessary to carry out the tests or inspections.

The right to demand information or admittance to premises and aids pursuant to the second and third paragraphs shall apply notwithstanding any obligation of professional secrecy.

The supervisory authorities and other persons who are in the service of the supervisory authorities shall be subject to provisions of professional secrecy pursuant to section 15. The obligation of professional secrecy shall also apply to information concerning security measures.

The King may prescribe regulations regarding exemptions from the first to fourth paragraphs in the interests of the security of the realm. The King may also issue regulations concerning the reimbursement of expenses incurred in connection with inspections. Recovery of any amount outstanding in the reimbursement of such expenses may be enforced by execution.

Amended by Act of 29 August 2003 no. 87 (effective 1 Sept 2003 by Royal Decree of 29 Aug 2003 no. 1092).

Section 32 Authorization to issue orders

The Data Inspectorate may issue orders to the effect that the processing of personal health

data which is contrary to provisions laid down in or pursuant to this Act shall cease, or impose conditions which must be fulfilled in order for the processing of the personal health data to be in compliance with this Act. If, furthermore, it must be assumed that the processing of personal health data may have adverse consequences for patients, the Norwegian Board of Health may issue such orders as mentioned. When the Data Inspectorate has issued an order, the Norwegian Board of Health shall be informed accordingly. When the Norwegian Board of Health has issued an order, the Data Inspectorate shall be informed accordingly.
Orders pursuant to the first paragraph shall include a time limit for compliance with the order.
Decisions made by the Data Inspectorate in pursuance of sections 26, 28, 31, 32 and 33 may be appealed to the Privacy Appeals Board.

Section 33 Coercive fine

In connection with orders pursuant to section 32, the Data Inspectorate may impose a coercive fine which will run for each day from the expiry of the time limit set for compliance with the order until the order has been complied with.
The coercive fine shall not run until the time limit for lodging an appeal has expired. If the administrative decision is appealed, the coercive fine shall not run until so decided by the appeals body.
The Data Inspectorate may waive a coercive fine that has been incurred.

Section 34 Penalties

Any person who wilfully or through gross negligence violates section 13a shall be liable to fines or imprisonment for a term not exceeding three months.

Any person who wilfully or through gross negligence:

1. processes personal health data contrary to sections 16 or 18,
2. omits to provide information to the Data Subject pursuant to sections 23 or 24,
3. omits to send notification to the Data Inspectorate pursuant to section 29,
4. omits to provide information to the Supervisory Authorities pursuant to section 31, or
5. omits to comply with orders of the Supervisory Authorities pursuant to section 32,

shall be liable to fines or imprisonment for a term not exceeding one year or both.

In particularly aggravating circumstances, a sentence of imprisonment for a term not exceeding three years may be imposed. In deciding whether there are particularly aggravating circumstances, emphasis shall be placed, *inter alia* on the risk of great damage or inconvenience to the Data Subject, the gain sought by means of the violation, the duration and scope of the violation, manifest fault, and on whether the Data Controller has previously been convicted of violating similar provisions.

An accomplice shall be liable to similar penalties.

In regulations issued pursuant to this Act, it may be prescribed that any person who wilfully or through gross negligence violates such regulations shall be liable to fines or imprisonment for a term not exceeding one year or both.

Amended by Act of 9 May 2008 no. 34 (effective 9 May 2008 by Royal Decree of 9 May 2008 no. 442).

To be amended by Act of 20 May 2005 no. 28 (effective from such time as laid down by law) as amended by Act of 19 June 2009 no. 74.

Section 35 Compensation

The data controller shall compensate damage suffered as a result of the fact that personal health data have been processed contrary to provisions laid down in or pursuant to this Act, unless it is established that the damage is not due to error or neglect on the part of the controller.

The compensation shall be equivalent to the financial loss incurred by the injured party as a result of the unlawful processing of the personal health data. The controller may also be ordered to pay such compensation for damage of a non-economic nature (compensation for non-pecuniary damage) as seems reasonable.

Chapter 7 Relationship to other statutes. Commencement.

Section 36 Relationship to the Act relating to the Processing of Personal Data

Insofar as it is not otherwise provided by this Act, the Personal Data Act and appurtenant regulations shall apply as supplementary provisions.

Section 37 Commencement

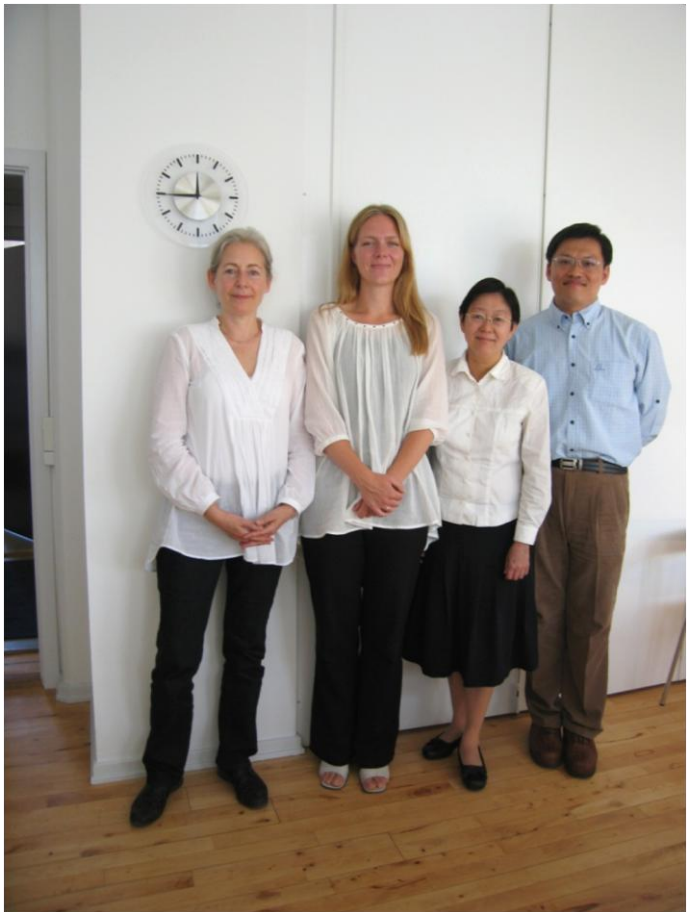
This Act shall enter into force from the date decided by the King. The King may decide that the individual provisions of the Act shall enter into force on different dates.

Section 38 Amendments to other statutes

附錄四、參訪過程剪影

與 Danish National Board of Health 接待同仁合影

Statistics Denmark 很有特色的大門



與 Danish Data Protection Agency 接待同仁合影

在 Director of the Division of Epidemiology Per Magnus 的辦公室與其合影

與 Executive Director Bjorn Henrichsen 及兩位 Deputy Director 合影