联合国 A/74/277

大 会

Distr.: General
5 August 2019
Chinese
Original: English

第七十四届会议

临时议程* 项目 72 (b)

促进和保护人权：人权问题，
包括增进人权和基本自由
切实享受的各种途径

隐私权

秘书长的说明

秘书长谨向大会转交隐私权问题特别报告员约瑟夫·卡纳塔西根据人权理事会第 28/16 号决议编写并提交的报告。

* A/74/150。

19-13343 X (C) 230819 290819

隐私权问题特别报告员的报告

摘要

本报告由隐私权问题特别报告员约瑟夫·卡纳塔西根据人权理事会第 28/16 号决议编写并提交。

报告载有活动摘要和关于保护和使用健康相关数据的建议书。

一. 活动摘要

1. 自 2018 年 10 月以来，隐私权问题特别报告员访问了德国、阿根廷和大韩民国，并将就此于 2020 年向人权理事会报告。除其他事项外，监督工作已展开，国际情报监督论坛已于 2018 年在马耳他举行，并将于 2019 年在伦敦举行。特别报告员感谢东道国政府对这些活动的支持，这些活动促成制定一项必须适用于国际情报数据交换的原则："如可传输，则可监督"。特别报告员编写了一份关于性别问题的报告草稿以及关于隐私及儿童和隐私衡量标准的准则，该报告草稿将提交于 2019 年 10 月 30 日和 31 日在纽约举行的磋商会。他还编写了载于本报告附件的建议书。特别报告员对欧洲委员会于 2019 年 6 月共同主办健康相关数据磋商会议表示感谢。

二. 健康相关数据

2. 以下文书承认人人有权享有可达到的最高标准的身心健康:《世界人权宣言》(第二十五条)以及《经济、社会及文化权利国际公约》(第十二条)、《儿童权利公约》(第 24 条)、《消除对妇女一切形式歧视公约》(第十二条)和《残疾人权利公约》(第二十五条)等国际人权文书。

3. 人们日益认识到健康相关数据的敏感性。在数字时代，此类数据经常在未经相关个人同意或知悉的情况下，以各种方式被获取和使用。收集和使用健康相关数据的产业以及日益增多的数据泄露事件都引起了极大关注。

4. 正是在这种背景下，特别报告员于 2017 年成立了隐私和保护健康相关数据工作队，负责编写一份关于保护和使用健康相关数据的建议书，供会员国用作健康相关数据最低数据保护标准的国际基线。该建议书纳入了全球磋商的结果和利益攸关方的数百条评论意见。

5. 该建议书是在工作队秘书 Sean McLaughlan 的协调下起草的，由主席 Nikolaus Forgó 指导，并得到工作队以下成员的贡献：Teki Akuetteh Falconer、Heidi Beate Bentzen、Elizabeth Coombs、Kenneth W.Goodman、Trix Mulder、Katerina Polychronopoulos、Chris Puplick、Mariana A. Rissetto、William Smart、Sam Smith、Jane Kaye、Steve Steffensen、Thomas Trezise、Melania Tudorica,、Marie-Catherine Wagner 和 Helen Wallace。

6. 该建议书的基础是，不论残疾、性别、性别认同、性别表达或其他因素如何，人人都有权获得可达到的最高标准的身心健康，并有权使自身健康相关数据获得可达到的最高标准的保护。强调同意保护人的尊严和完整，同时规定使用符合公共利益(如科学研究)的健康数据享有适当的保障。

7. 附件所载为缩略版的建议书，着重指出了关键要素。在将其转化为国内法时，各国应使用完整版，完整版可查阅 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf。

附件

关于保护和使用健康相关数据的建议书

第一章

总则

1. 宗旨

1.1 本建议书的目的是就健康相关数据的数据处理提供指导原则。

1.2 该指导意见将作为健康相关数据最低数据保护标准的国际基线。

2. 范围

2.1 本建议书适用于社会所有部门(包括公共和私营部门)对健康相关数据的数据处理。

2.2 本建议书不限制或以其他方式影响比其准予更多数据主体、更广泛或更好的权利、保护和/或补救措施的任何法律。

2.3 本建议书不适用于个人在纯粹的个人或家庭活动中进行的健康相关数据处理。

3. 定义

- “匿名化”指对个人数据采取的一种不可逆过程，使得在任何情况下或通过任何直接或间接的方式(包括使用其他数据或与其他数据链接)均不能识别数据主体。
- “主管监督机关”指一个独立的公共机关，其职责是单独或连同其他目的监督本建议书条款的实施和遵守情况。
- “同意”指明确的肯定行为，例如通过书面声明(包括通过电子手段)或口头声明，就数据主体同意处理与其有关的个人数据自由作出具体、知情和明确的表示。这可能包括在访问网站时勾选一个方框，对提供信息社会服务选择技术设置，或用另一个声明或行为，明确表示在这种情况下数据主体接受对其个人数据的拟议处理。因此，沉默、预先勾选框或不活跃状态不应表示同意。同意应涵盖出于同一个目的或多个目的而进行的所有处理活动。当处理有多个目的时，每个目的都应该得到同意。如果数据主体的同意是在提出请求后以电子方式作出的，则请求必须明确、简洁且不对使用所请求的服务造成不必要的干扰。
- “控制者”是指单独或与他人共同拥有健康相关数据处理方面决策权的自然人、法人、公共机关、服务提供者、机构或任何其他组织。

- “数据处理”指对个人数据进行的任何一项或一组操作，例如收集、记录、组织、构建、存储、销售、保存、改编或更改、检索、访问、咨询、使用、披露、传播、提供、共享、排列或组合、限制、擦除或销毁数据，或对个人数据进行逻辑和/或算术运算，以及自动处理健康相关数据。

- “数据主体”指已识别或可识别的自然人。可识别的自然人是可以直接或间接识别的人，特别是通过参考姓名、身份号码、位置数据、网络标识符等标识符或该自然人的身体、生理、遗传、心理、经济、文化或社会身份特有的一个或多个因素来识别。

- “残疾”是一个不断演变的概念；残疾是伤残者和阻碍他们在与其他人平等的基础上充分和切实地参与社会的各种态度和环境障碍相互作用所产生的结果。残疾人包括肢体、精神、智力或感官有损伤的人，这些损伤与各种障碍相互作用，可能阻碍残疾人在与他人平等的基础上充分和切实地参与社会。

- “检查”包括任何具有非临床、诊断或预测价值的非基因检测或基因检测。如果检查结果证实或否定对某人疾病的诊断，则该结果具有诊断价值。如果检查结果表明未来有生病的风险，则该结果具有预测价值。具有预测价值的检查结果的可靠性有很大差异。检查还包括执法机关使用的检查(例如，用于当前调查或预测性调查的 DNA 筛检)。

- “基因数据”指在产前发育期间遗传或获得的与个人遗传特征有关的所有个人数据，因为这些数据是通过对有关个人的生物样本进行分析得出的，特别是染色体、DNA 或 RNA 分析或对任何其他能够获得等效信息的元素的分析。DNA 的遗传性意味着对个人 DNA 的分析也可能对其他亲属、群体和人群产生影响。基因数据包括关于个人表现型的信息。

- “基因检测”指为分析人类起源的生物样本而进行的检测，具体目的是确定一个人在产前早期发育过程中遗传或获得的遗传特征。在基因检测背景下进行的分析是对染色体、DNA 或 RNA 或任何其他能够获得等效信息的元素进行分析。

- “卫生信息系统”指为决策提供基础并具有数据生成、汇编、分析、存储和合成以及通信和使用等一系列功能的系统。卫生信息系统从卫生部门和其他相关部门收集数据、分析数据，确保数据的总体质量、相关性和及时性，并将数据转化为供保健相关决策使用的信息。[1]

- “健康相关数据”指与个人的身体或心理健康包括保健服务提供情况有关的所有个人数据，这些数据揭示了有关个人过去、现在和未来健康状况的信息。基因数据在本建议书中可理解为健康相关数据。健康相关数据涉及但不限于通过产前诊断、移植前诊断等检测或通过遗传特征识别产生的数据，无论是

[1] 世界卫生组织，《国家卫生信息系统框架和标准》，第 2 版(2008 年)。

否被视为母亲的健康相关数据，都必须受到与其他健康相关数据同等程度的保护。

- “健康相关数据泄露”指意外或非法破坏、丢失、更改、未经授权披露、访问或阻止合法访问(包括非法锁定做法）或出售所传输、存储或以其他方式处理的健康相关数据；这不包括蓄意合法破坏。
- “卫生工作者”指所有参与以增进健康为主要目的的行动的人。
- “人道主义行动”指为应对人道主义紧急情况而在公正的基础上进行的援助、救济和保护活动。人道主义行动可包括人道主义援助和保护。[2]
- “土著数据”指以任何形式或媒介呈现的关于、来自或可影响土著人民或原生民族人民集体或个人的数据、信息或知识，可包括土著人民的语言、文化、基因数据、环境或资源。
- “土著数据主权”指土著人民在创建、收集、访问、分析、解释、管理、传播、重新使用和控制与土著人民有关的数据方面所享有的固有权利和利益。
- “土著数据治理”指土著人民自主决定收集、获取和使用土著数据的内容、方式和原因的权利。它确保关于土著人民的数据反映土著人民的优先事项、价值观、文化、世界观和多样性。这包括土著人民对土著数据行使控制权的原则、结构、问责机制、法律文书和政策。
- “被保险人”指计划或者已经订立保险合同的个人，也适用于由公共保险或法定保险承保的个人。
- “承保人”指私营公司、社会保障机构和再保险公司。
- “国际组织”指受国际公法管辖的组织及其下属机构，或由两个或两个以上国家设立或依照国家间协定产生的任何其他机构。
- “互操作性”指不同信息系统之间通信和交换数据的能力。
- “交集性”指适用于特定个人或群体的社会分类(如种族、阶级和性别)的互联性，社会分类被认为创造了彼此重叠和相互依存的产生歧视或弱势群体的系统。
- “医学算法”指用于帮助做出保健决定或分析健康信息的基于软件或计算机的算法，包括人工干预算法和无人干预算法。
- “移动应用程序”指在移动环境中可用于促成健康相关数据交流和管理的手段。其包括不同的形式，例如出于预防、诊断、监测、治疗、娱乐或健康目的可使用的软件、可穿戴式联网医疗和保健物品和设备。

[2] Christopher Kuner and Massimo Marelli, eds., *Handbook on Data Protection in Humanitarian Action* (International Committee of the Red Cross, 2017).

- “开放数据”指不受位置或用途限制可供使用和共享，并且与可识别的个人无关的数据。开放数据可以由任何人在任何地点出于任何目的自由使用、共享和构建；它们可以方便和可修改的形式免费提供，并在允许重用和重新分配的条件下提供，包括人人可不受限制地将与其他数据集混合使用和互相操作。

- “个人数据”指与已识别或可识别的自然人(“数据主体”)有关的任何信息。

- “处理者”指仅在代表控制者并根据控制者指示时，才单独或与他人一起处理数据的自然人或法人、公共机关、代理机构或任何其他机构。

- “配置文件”指旨在应用于个人的一套表征一类人的健康相关数据。

- “数据配置”指任何形式的自动处理健康相关数据，包括使用健康相关数据来评估与自然人有关的某些个人数据，特别是分析或预测与该自然人的工作表现、经济状况、健康、个人偏好、兴趣、可靠性、行为、位置或移动有关的数据。

- “假名化”是指按以下方式处理个人数据，即在不使用单独保存的附加信息的情况下，不能再将个人数据归属于特定的数据主体，以及由于受技术和组织措施的制约，从而个人数据不能归属或不可归属于已识别或可识别的个人。假名化数据仍然是个人数据。

- “建议书”指本文件。

- “参考框架”指经过更新、适合实践、适用于卫生信息系统，并且涵盖互操作性和安全性领域的一系列协调规则和/或流程。

- “科学研究”指为增加知识存量和/或为现有知识设计新应用而进行的创造性和系统性工作。该活动必须是新颖、具有创造性的、不确定、系统性的，可转移和/或可复制的。确定一项活动是否为科学研究的因素包括：开展该活动的法律实体的作用；开展该活动的自然人的作用；质量标准，包括科学方法和科学出版物的使用；以及对研究道德规范的遵守情况。任何可以处理健康相关数据的学科内研究，包括医学和保健科学、自然科学、工程和技术、社会科学、人文艺术，都是科学研究。科学研究可以是基础研究、应用研究或实验开发。政策分析、保健服务和流行病学都是科学研究的例子。科学研究既可以由政府、也可以由私人资助和进行，在某些情况下可能是为了盈利而进行的。

- “跨界”指跨越国家边界，包括跨越国家内部的次国家边界。只要数据跨越国家边界传输，如位于同一国家的发送者和接收者之间传输的数据通过另一个国家发送，或者一人或多人已经或在某些条件下可能已经从另一个国家远程访问数据，就会发生跨界数据传输。

第二章

健康相关数据处理的法律条件

4. 健康相关数据处理的原则

4.1 处理健康相关数据必须遵循以下原则：

(a) 必须以一种透明、合法和公平的方式处理健康相关数据；

(b) 收集健康相关数据必须出于明确、具体和合法的目的，并且健康相关数据的处理方式必须与最初收集数据的目的相符。出于符合公共利益的归档目的、科学或历史研究目的或统计目的进一步处理不应被视为与最初目的不相符，且应为数据主体的权利和自由提供适当保障；

(c) 健康相关数据的处理应是必要的，并仅限于根据第 5 条所追求和进行的合法目的；

(d) 在可能的情况下，必须从数据主体收集健康相关数据。如果数据主体不能提供数据，而此类数据对于健康相关数据的数据处理是必要的，则可根据第 5 条从其他来源收集这些数据；

(e) 健康相关数据必须是充分的、相关的、准确的、最新的并且仅限于数据处理用途，并且必须适合用于数据处理用途；

(f) 必须有足够的安全和组织措施来处理健康相关数据。保障措施必须保证尊重数据主体的权利和健康相关数据的安全。依法可以提供任何其他保障，保障对数据主体及其健康相关数据的权利和基本自由的尊重；

(g) 必须尊重其健康相关数据参与任何数据处理实例的数据主体的权利。这包括但不限于访问数据、信息、纠正、反对、擦除和数据可移植性的权利。数据主体有权请求将其由自动处理系统保留的健康相关数据和/或打印文本档案或记录，以合理的成本在技术可行的地方传输给数据主体选择的另一实体。

4.2 必须默认考虑健康相关隐私原则(默认隐私)，并将其纳入信息系统的设计中(设计隐私)。

4.3 必须定期审查对个人数据和健康相关数据的所有适用原则的遵守情况，包括但不限于本建议书中的原则。控制者必须在开始处理数据之前和此类处理之后定期对处理数据在数据保护、数据使用和尊重数据主体隐私方面的潜在影响进行书面评估，包括减少所有风险的措施。

4.4 控制者和处理者必须采取一切适当措施，履行其在健康相关数据方面的义务，包括但不限于本建议书中的义务，并且必须能够向主管监督机构证明，健康相关数据的所有数据处理正在或已经按照所有适用的义务进行。

4.5 不受特定专业保密级别限制的控制者和处理者必须确保健康相关数据的所有数据处理都按照保密规则和安全措施进行，以便保护水平相当于针对卫生工作者实施的保护水平。

5. 健康相关数据处理的法律依据

5.1 如果健康相关数据处理第 4 条且数据处理是必要的；根据本建议书所述原则进行，并适用下列情况之一，则该数据处理是合法的：

(a) 数据主体已对该数据处理给予其自由、具体、知情和明确的同意，除非法律禁止数据主体同意数据处理。如果法律不排除数据主体同意的要求，则必须在要求数据主体同意时，告知其有权随时撤回对数据处理的同意，并告知，任何这种撤回同意的行为不会影响在撤回同意之前已经在其同意的基础上进行的任何数据处理的合法性。任何数据主体撤回同意必须与给予同意一样容易。必须为数据主体提供可理解的、清晰的、全面的相关信息，以供其作出同意决定或不作出同意决定。在处理或以其他方式使用数据主体的健康相关数据之前，数据主体有知情同意权；

(b) 用于履行数据主体为当事人的合同，或为了在订立合同前应数据主体的请求采取措施；

(c) 履行控制者所承担的法律义务；

(d) 保护数据主体或者其他自然人的重大利益；

(e) 为公共利益或行使赋予控制者的官方权力而执行的任务；

(f) 用于控制者或第三方追求的合法利益，除非需要保护个人数据的数据主体的利益或基本权利和自由高于此等利益，特别是在数据主体是儿童的情况下；

(g) 第(f)点不适用于公共机关在执行任务时进行的处理。

5.2 处理健康相关数据的合法目的是：

(a) 对数据主体直接有益，例如数据主体的健康诊断、护理、治疗、康复和恢复；

(b) 预防保健的目的和保健诊断的目的、卫生工作者以及社会和医疗-社会部门人员在遵守法律规定的条件下的保健或治疗管理或保健服务管理；

(c) 在符合法律规定的条件下，出于公共卫生的理由，例如强制通报的疾病、健康危险防护、传染病的识别和遏制、环境危害、人道主义行动或为了达到医疗质量和安全的高标准、保健产品和医疗器械的防护；

(d) 在无法获得数据主体、其他个人或两者的同意时，保障数据主体或其他个人的重大利益；

(e) 根据法律或任何合法的集体协议，出于与控制者的义务相关的理由，以及与行使数据主体在就业和社会保护方面的权利相关的理由；

(f) 在符合法律规定的条件下，出于对卫生保健服务的规划、筹资和管理问责中的公共利益，对社会福利和医疗保险福利和服务的索偿管理；

(g) 出于法律规定的符合公共利益的归档目的、科学或历史研究目的进行的处理，参照开展活动的法律实体的作用、开展活动的个人的作用、质量标准进行评估，包括科学方法的使用和科学出版或统计目的，符合法律规定的条件，以保证对数据主体的基本权利和合法利益的保护(见第五章“适用于为科学研究处理健康相关数据的条件”)；

(h) 对承认、行使或抗辩拟与用于数据处理的健康相关数据相关的法律索赔至关重要；

(i) 根据规定保障数据主体及其亲属的权利和利益的适当和具体措施的法律，该处理对于确认失踪人员或其位置至关重要(没有理由相信该个人只是希望避免接触)并且该情况引起了对失踪人员安全和福祉的关注。

5.3 可对数据主体明显公开的健康相关数据进行数据处理，除非此类处理与本建议书规定的数据主体的权利相矛盾或受到其他法律保障(如用于保险目的)。数据主体在社交媒体上向其联系人传递的信息不属于明显地公开健康相关数据。

6. 儿童健康相关数据

6.1 与儿童有关的健康相关数据和基因数据必须至少受到与其他健康相关数据同等程度的保护。只要知情同意是处理儿童个人数据的法律基础，儿童就有权被告知，并且必须考虑到未成年人充分理解处理结果以及任何适用法律的能力。

6.2 一旦儿童达到法定成年年龄，应寻求其同意(或重新同意)才能参与研究。

6.3 当儿童达到法定成年年龄时，他们有权从任何卫生信息系统中撤回健康相关数据。

7. 基因数据

7.1 基因数据的数据处理只能在符合适当保障措施的情况下进行，并且根据法律规定，或根据第 5.2 款在数据主体同意的基础上进行，除非法律规定数据主体不能和/或不需要对其基因数据的任何处理表示同意。

7.2 与数据主体或其血亲有关的出于预防、诊断或治疗目的而进行的基因数据处理，或用于科学研究的基因数据处理可被用于数据处理的特定目的；或者使得与这种基因数据处理结果有关的人员能够做出知情决定，但不会在那些与结果有关的人尚不清楚他们与数据主体的关系时向他们透露此种关系的性质。在达到这些目的后，必须在没有数据主体同意的情况下销毁基因数据。

7.3 来自基因检测的现有预测数据不得用于其他目的，包括保险或执法目的，除非必要和相称的法律特别规定。

7.4 数据主体有权知道或不知道由基因数据的数据处理产生的与其基因数据有关的信息。在进行任何数据处理之前，必须告知数据主体可能不被告知结果，包括任何偶然发现。

8. 为提供和管理卫生保健而共享健康相关数据

8.1 如果健康相关数据由一名卫生工作者转交给另一名卫生工作者以提供和管理个人的卫生保健，则应在披露之前通知该个人，除非由于紧急情况或根据第11.4款，这一条件无法满足。

8.2 除非法律规定了适当的保障措施，否则健康相关数据只能传达给受保密规则约束的授权接收人。

8.3 卫生工作者之间的数据交换和披露必须仅限于个人的护理、预防或医疗-社会和社会后续跟进的协调或连续性所需的信息。卫生工作者应能够披露或接收为护理病人和履行其职责所需的健康相关数据。

8.4 在健康相关数据的交换和披露中，必须采取实体、技术或行政安全措施以保证健康相关数据的机密性、完整性、真实性和可用性。

9. 为提供和管理卫生保健以外的目的披露健康相关数据

9.1 健康相关数据可以向法律授权和要求可获得和拥有该数据的接收人披露，以促进或开展对健康问题的研究；规划、改善和管理保健系统；和/或制定、评估或监测保健活动和方案。只有在法律规定的必要和相称的标准下，才能授权此类处理。

9.2 保险公司、雇主和承包商不能被视为经授权可获得个人健康相关数据的接收人，除非法律规定了适当的保障措施并且符合第5条。

10. 健康相关数据的存储

10.1 健康相关数据的存储时间不得超过收集健康相关数据的用途所需的时间。

第三章

数据主体的权利

11. 处理透明权

11.1控制者必须告知数据主体所具有的公平、透明地处理其健康相关数据的权利，具体而言：

(a) 控制者和任何处理者的身份和详细联系方式；

(b) 正在处理的健康相关数据的来源(如适用)；

(c) 有关健康相关数据的类别；

(d) 处理的目的，以及处理该健康相关数据的法律依据；

(e) 存储健康相关数据的时长，或者如果无法明确，则应告知决定时长的标准；

(f) 健康相关数据的接收人或接收人类别，以及向获得健康相关数据的国家以外的国家或国际组织(该情况下，数据只能传输到接受该数据的国际组织)计划传输健康相关数据，此种传输应遵守本建议书的条款；

(g) 在适用的情况下，反对在第 12.2 款所述条件下处理健康相关数据的可能性；

(h) 可用于行使访问、纠正和删除健康相关数据的权利的条件和手段；

(i) 根据法律规定的适当保障措施并符合第 4.1 (b)款所述的条件，如果其健康相关数据的处理是出于协调目的或符合公共利益的存档目的、科学或历史研究目的或统计目的，此数据处理可随后发生；

(j) 可能存在涉及健康相关数据的自动化决策，包括数据配置，这仅在符合法律规定并有适当保障措施的情况下才可发生；

(k) 预期数据处理的任何风险，以及健康相关数据泄漏时可用的补救措施；

(l) 关于处理其健康相关数据的投诉机制，包括在数据处理发生的每个管辖区中向谁提出此类投诉；

(m) 数据保护官员或数据控制者的身份和详细联系方式，数据主体可向其寻求与健康相关数据的拟议数据处理有关的进一步信息；

(n) 健康相关数据的数据处理可能涉及的拟议管辖区，以及数据主体将拥有的相对于这些权利的权利。

11.2 必须在健康相关数据的数据处理之前提供第 11.1 款中规定的信息。

11.3 信息必须是可理解的、易于获取的、使用通俗语言并合时宜的，确保数据主体能够完全理解。

11.4 在以下情况中，不要求控制者提供第 11.1 款中的信息：

(a) 数据主体已经拥有该信息；

(b) 允许不直接从数据主体处收集健康相关数据；

(c) 此类健康相关数据的数据处理由法律明确规定；

(d) 无法联系到数据主体。

11.5 如果健康相关数据的数据处理是为了符合公共利益的存档目的，并且无法联系到数据主体，则可在进行数据处理之前健康相关数据是假名或匿名的条件下为这些目的进行数据处理，除非法律另有规定。

12. 获取健康相关数据、健康相关数据的可移植性、纠正和擦除以及反对处理健康相关数据

12.1 数据主体有权知道与其有关的健康相关数据的处理是否正在进行，如果正在进行，有权在没有过多延迟或费用的情况下，以可理解的形式得知其健康相关数据，并在相同条件下至少可获得以下信息：

(a) 处理健康相关数据的一种或多种目的；

(b) 有关健康相关数据的类别；

(c) 健康相关数据的接收人或接受人类别和设想的数据传输到第三国/多国或一个/多个国际组织；

(d) 健康相关数据的数据处理将发生的时间段，包括存储期；

(e) 对健康相关数据进行数据处理的基本理由是，此类数据处理的结果适用于数据主体，包括数据配置，这仅在法律规定并符合适当保障措施的情况下可以开展。

12.2 数据主体有权：

(a) 擦除处理方式与本建议书相悖的健康相关数据；

(b) 纠正不准确或误导性的健康相关数据；

(c) 以与其生活和福祉有关的理由反对对其健康相关数据进行数据处理。在法律授权控制者对健康相关数据进行数据处理的情况下，尽管有异议，控制者必须以不能识别数据主体的方式将拟议的数据处理和数据主体提出的反对通知主管监督机关(除非数据主体同意被识别)。

12.3 如果纠正或擦除被拒绝，数据主体必须能够审查该决定，并且在发生健康相关数据泄露时有权获得适当的补救。

12.4 数据主体有权不服从仅基于对其产生重大影响的自动处理(包括数据配置)作出的健康相关数据决定。只有与所追求的目标、尊重数据保护权、隐私权以及为保护数据主体的基本权利和自由提供适当和具体保障措施相称的法律，才能允许免除这一禁令。出于健康目的数据配置应符合普遍接受的科学有效性、临床有效性和临床实用性标准，并应遵守适当的质量保证方案。

12.5 受法律规定的条件的约束，在健康相关数据的数据处理是通过自动手段进行的情况下，数据主体可以结构化、可互操作和机器可读的格式从控制者处获得关于其健康相关数据的传输信息，从而将该健康相关数据传输给另一控制者。数据主体也可要求控制者将其健康相关数据从速直接传输给指定的控制者。

12.6 数据主体的权利可受法律规定的限制，而该法律构成符合以下利益的必要和相称措施：

(a) 保护国家安全、公共安全、国家经济利益或者制止刑事犯罪；

(b) 保护数据主体或他人的权利和自由，并提供适当的保障措施，确保尊重数据主体的权利。

第四章

安全性和互操作性

13. 安全性

13.1 健康相关数据的数据处理必须安全进行。

13.2 系统可用性，即包含健康相关数据的系统正常运行，必须通过能够使健康相关数据以一种安全的方式获取的措施加以提升，并适当考虑授权人员的许可级别。

13.3 保证健康相关数据处理的完整性需要能够对健康相关数据的处理行为进行验证的机制；建立监测健康相关数据的获取和使用的措施，以确保只有经授权的人员才能获取、使用和数据处理健康相关数据。包含健康相关数据的系统必须是可检查的，以便能够识别进行任何特定操作或数据处理的用户。

14. 互操作性

14.1 互操作性必须完全符合本建议书中规定的原则。

14.2参考框架提供了促进互操作性的技术框架，必须保证高度安全性并定期检查。

第五章

科学研究

15.1 为开展科学研究而对健康相关数据进行的处理应得到法律规定的适当保障，遵守本建议书的规定，尊重数据主体的任何其他权利和基本自由，且必须有合法理由。未经事先自由、具体和知情同意，不得要求或强迫任何个人参加科学研究。

15.2 同意参与研究并不等同于同意对数据进行处理。为科学研究进行健康相关数据处理的条件，必须在处理数据之前由包括非专业成员在内的独立主管机构(例如，道德委员会或独立数据保管人)进行评估。这种评估将接受主管监督机关或其他道德委员会又或者其他独立数据保管人的审查，以确保其符合批准条件和批准事实。

15.3 根据本建议书第 15.5 款，除了同意参与研究外，还需要单独的合法依据才能处理数据。科学研究中数据处理的合法依据可以是但不一定是同意：要么是因为无法满足有效同意处理数据的条件，要么是因为数据处理是法律规定的。

15.4 必须根据以下内容评价是否需要对用于科学研究的健康相关数据进行数据处理：科学研究的目的、科学知识、尊重道德准则、所谓的效益、对数据处理的限制、数据主体将面临的风险、群体伤害的风险，以及就基因数据而言，与数据

主体共享某些基因数据的血亲将面临的风险，以及发现非亲子关系或其他意外家庭关系的风险。只能在必要和相称的情况下才能减损患者参与研究的权利。

15.5 按照第 5.2 款，只有在数据主体同意的情况下，才能在科学研究项目中对健康相关数据进行处理，除非法律另有规定。任何规定在未经数据主体同意的情况下为科学研究处理健康相关数据的法律必须是：必要的、相称的且符合公共利益；尊重数据保护权；并规定适当和具体的保障措施，以保护数据主体的权利和自由。这些保障措施应确保根据第 4.1(e)款遵守数据最小化原则，且可包括技术和组织措施。

15.6 除第三章(包括但不限于第 11.1 款)的要求外，数据主体还必须在以下方面事先获得尽可能准确的透明且可理解的信息：

(a) 科学研究的性质、数据主体可使用的备选办法以及使用健康相关数据的任何相关条件，包括可能的再次联系和结果/发现的反馈；

(b) 提取新形式的健康相关数据的手段和能力，以及未来可提取数据的不确定性；

(c) 健康相关数据存储的适用条件；

(d) 法律规定的权利和保障措施，特别是数据主体拒绝同意为科学研究而处理数据的权利和随时根据第 5.2 款撤回同意参与研究的权利，此外，根据第 15.11 和 15.12 款，销毁在撤回同意前已经分析和/或公布的健康相关数据可能是不可行的；

(e) 研究的目的、方法、供资来源、任何可能的利益冲突、研究人员所属的机构、预期效益和潜在风险，以及研究可能带来的不适、研究后规定和研究的任何其他相关方面；

(f) 将受权获取数据或可能出于其他目的合法寻求获取数据的第三方的身份，以及如何限制这些目的；

(g) 有计划的跨国数据传输，包括根据第 17.1 款进行传输的法律依据；

(h) 拟议发布的健康相关数据，以及任何设想在研究数据储存库中存储的数据。

15.7 如果满足第 11.4 或 11.5 款的条件，则控制者无须直接向每个数据主体提供信息。不过，当第 11.4 或 11.5 款适用时，应以可公开查阅的方式向数据主体提供信息。

15.8 对于在收集时无法确定数据处理具体目的的科学研究，数据主体应能够同意在预期目的允许的范围内，在遵守公认道德标准的情况下，对某些研究领域、研究项目的某些部分或出于建立生物数据库之目的进行数据处理。当有可能进一步说明用途时，应根据第 11.1、15.6 和 15.7 款告知数据主体。可使用数字动态同意来实现这些目的。这项规定绝不会减少第 5.2 款对同意的要求，因为那些要求适

用于科学研究。数据主体也可以预先同意未来可在其死亡后将其健康相关数据用于科学研究。

15.9 持有健康相关数据的科学家在其拥有或控制健康相关数据时，将对任何数据泄露承担责任。在其他科学家可以获得健康相关数据之前，必须制定法律确定的补充保障措施，例如要求获得法律指定的主管机构的明确同意或评估。

15.10 在技术上切实可行的情况下，健康相关数据必须匿名。在不能从技术上切实可行地进行匿名化处理的情况下，应对健康相关数据进行假名化处理，即在识别数据分离阶段由可信第三方进行干预，以保障数据主体的权利和基本自由。控制者不能同时充当可信第三方。这必须在能够通过对不允许或不再允许识别数据主体的健康相关数据做进一步处理来实现科学研究目的情况下进行。

15.11 若数据主体根据第 5.2 款的规定撤回同意或根据第 12.4 款反对处理数据，则必须按照数据主体的意愿销毁在该科学研究过程中处理的关于该数据主体的健康相关数据，除非违反法律。若销毁数据是违法的，则必须将此以及要求保留健康相关数据的法律告知数据主体。若数据的匿名化可以不影响研究的科学有效性但确保即使使用其他数据集也无法识别数据主体，则可以此作为销毁的替代办法，且应告知数据主体。若数据主体仍然要求销毁而不是对健康相关数据进行匿名化处理，则必须遵循其要求。若在处理健康相关数据有法律依据的情况下对这些数据进行分析，则销毁这些数据可能不可行，且可能损害科学研究数据集的完整性。在这种情况下，如果必须在符合公共利益的情况下开展科学研究以取得成果，或销毁数据将严重影响科学研究的科学有效性，则对健康相关数据的处理应严格限于实现这些目的所必需的数据，但不需要销毁数据。如果无法从已经进行的研究中删除数据，则不应将参与者的信息用于任何进一步研究。

15.12 用于科学研究的健康相关数据不得以能够识别数据主体的形式发布，但以下情况除外：

(a) 若数据主体已经同意，且该同意尚未撤回；

(b) 若法律允许发布，前提是这对于介绍研究发现不可或缺，且仅限于在发布数据的利益高于数据主体的利益、权利和自由的情况；

(c) 若数据主体撤回同意发布能识别该主体的健康相关数据，则数据控制者和/或处理者必须在可行的情况下销毁或删除健康相关数据。

第六章

移动应用程序

16.1 适用于本建议书中其他健康相关数据的法律保护和保密规定同样适用于移动应用程序收集的健康相关数据。

第七章

健康相关数据的跨境传输

17.1 健康相关数据的跨境传输只能在达到适当的数据保护等级时进行，或根据下列规定之一进行：

(a) 数据主体在获知适用的法律和因缺乏适当的数据保护保障水平而产生的风险后，明确、具体和自由地同意根据第 5.2 款传输数据；

(b) 在特定情况下，为了数据主体的具体利益需要进行此种传输；

(c) 传输符合法律规定的包括科学研究在内的重要公共利益，且传输是必要的、相称的措施；

(d) 就数据控制者追求的不低于数据主体的利益或权利和自由的普遍正当利益而言，必须进行传输，而且控制者评估了数据传输方面的所有情况，并在此评估的基础上为保护个人数据提供了适当的保障措施。控制者应将传输情况告知监督机关。控制者除须提供第 11.1 款提及的信息外，还须告知数据主体传输情况及其所追求的普遍正当利益；

(e) 传输构成一种实现表达自由的必要和相称的措施。

17.2 对于利用跨国云计算基础设施、平台或软件处理的健康相关数据，一国在根据国际法无义务行使管辖权时，只能在下列情况下行使管辖权：

(a) 该事项与力求行使管辖权的国家之间存在实质性联系；

(b) 力求行使管辖权的国家在该事项方面具有正当利益；

(c) 鉴于国家正当利益和其他利益保持平衡，行使管辖权是合理的。

第八章

电子健康记录

18.1 所有人都有隐私权，必须严格管理电子健康记录系统中健康相关数据的保密性和保护。

18.2 不能因个人没有电子健康记录而拒绝对其进行治疗。

18.3 数据主体可以选择防止向其他卫生工作者披露其在治疗期间由一名卫生工作记录的电子健康记录中的健康相关数据。

18.4 电子健康记录系统必须可以审核，并包含监控何人曾访问记录中的数据及其访问时长的电子协议、修改日志，以及确保不会未经授权访问且数据主体知晓何人曾访问其健康相关数据的协议。

18.5 需要有证据证明患者同意或撤回同意访问其电子健康记录中的数据的访问或撤回该同意的证据是必要的。必须以电子方式记录此种情况以便审核。

18.6 可为了进行科学研究和统计处理电子健康记录系统中的健康相关数据，只要这是达到为保护现行法律规定的个人权利而事先确定的特定目的所必需的。从电子健康记录系统中获取的健康相关数据必须以匿名形式用于研究。

18.7 数据主体必须有权访问其在电子健康记录系统中的健康相关数据。健康相关数据在电子健康记录中存储的时间不应超过其收集用途所需的时间。

18.8 必须定期审核并公开报告任何电子健康记录中的访问协议。

第九章

健康相关数据、基因数据和保险

19. 健康相关数据、基因数据和承保人

19.1 除非出于符合国际人权法的法律规定的重要公共利益原因，或者获得了数据主体的同意，否则不得向承保人披露基因数据。

19.2 出于科学研究之目的获得的健康相关数据和基因数据不能用于数据主体或其家庭成员的保险相关用途。

20. 承保人必须证明对健康相关数据进行处理是合理的

20.1 只可出于保险目的处理个人的健康相关数据，且须符合以下条件：

(a) 已指明处理目的，并已适当证明数据的相关性，且已告知数据主体数据处理的风险和合理性；

(b) 拟议进行的健康相关数据处理的质量和有效性符合公认的科学和临床标准；

(c) 预测性检查得出的数据具有高阳性预告值；

(d) 根据关于相关风险性质和重要性的相称原则，适当证明数据处理是合理的；

(e) 出于保险目的处理的健康相关数据的质量和有效性应符合公认的科学和临床标准。

20.2 除非法律特别授权，否则不得出于保险目的处理来自受保人家庭成员的健康相关数据。

20.3 出于保险目的对从公共领域获得的健康相关数据进行的处理不得评价风险或计算保险费。

21. **未经受保人或数据主体同意，承保人不得处理健康相关数据**

21.1 根据第 5.2 款，未经受保人同意，不得出于保险目的处理健康相关数据。

21.2 健康相关数据必须从受保人处收集。

22. **承保人必须为存储健康相关数据提供充分保障**

22.1 承保人不得存储收集用途不再需要的健康相关数据。若保险申请被拒绝或合同已经到期，不能再提出索赔，则保险公司不得存储健康相关数据，除非既必要又相称的法律要求存储这些数据。

23. **承保人不得出于保险目的要求进行基因检测**

23.1 不得出于保险目的进行预测性基因检测。

23.2 除非法律特别授权，否则不得出于保险目的处理基因数据检测得出的现有预测数据。在获得授权的情况下，只有在就所使用的检测类型和要投保的特定风险独立评估数据处理是否符合第 20.1 款中的标准后，才可以进行必要的数据处理。

23.3 不得出于保险目的处理受保人家庭成员基因检测得出的现有数据，且这些数据必须由承包人销毁。

24. **承保人应该考虑新科学知识**

24.1 承保人必须根据相关的新科学知识定期更新精算基础，并向任何受保人提供有关任何保险费的计算、保险费的额外增加或不在承保范围的任何全部或部分事项的信息和理由。

25. **各国应确保充分的调解、磋商和监测**

25.1 必须建立调解、磋商和监测程序，以确保公正和客观地解决争端，使各方之间的关系得到良好平衡，并能有力评价对本建议书的遵守情况，包括主管监督机关的遵守情况。

第十章

健康相关数据和雇主

26.1 健康相关数据的控制者可能包括雇主。任何此类雇主为任何健康相关数据泄露对数据主体负有责任。

26.2 雇主在向求职者提供工作前不得向其索取健康相关数据，但以下情况除外：

(a) 为了能够合理调整工作地点，以促进该求职者就业；

(b) 为了确定求职者是否能够履行相关工作固有的职能；

(c) 为了监测多样性并促进残疾人就业。

26.3 雇主必须告知雇员其权利以及处理其健康相关数据的目的。

26.4 雇员有权访问他们的医疗档案，以便能够核实其是否准确并纠正任何不准确或不完整的信息。

26.5 雇主必须确保雇员健康相关数据的保存时间不超过必要时间。

第十一章

健康相关数据和土著数据主权

27.1 土著人民和第一民族享有土著数据主权和土著数据治理权。

第十二章

健康相关数据和开放数据

28.1 未经可能受影响的每个人事先、知情、具体同意，不得将单元记录级别的健康相关数据作为开放数据发布，也不得将假名化的数据作为开放数据发布。就基因数据而言，可能受影响的个体包括提议披露其基因数据之人的血亲。

28.2 如果将健康相关数据作为开放数据发布并由此导致健康相关数据泄露，则处理健康相关数据的一方和将其作为开放数据发布的一方(若两者不相同)均对数据主体负有责任。

第十三章

健康相关数据和自动化决策

29.1 数据主体应有权不服从仅基于对其产生重大影响的健康相关数据自动处理(包括数据配置)作出的决策。数据主体还应有权让人对自动处理作出的原有决定进行审查及再次作出决定。

29.2 如果决定符合以下情况，则第 29.1 款不适用：

(a) 对于数据主体和数据数据控制者签订或履行合同是必要的；

(b) 是经数据控制者必须遵守的一项法律授权的，该法律规定了维护数据主体权利和自由以及正当利益的适当措施；

(c) 基于数据主体的明确同意，并且数据主体在同意之前知晓，如果同意，则将失去进行人工审查和重新作出决定的权利。

29.3 如果第 29.2 款的(a)或(c)项适用，控制者应采取适当措施，保障数据主体的权利、自由和正当利益。

第十四章

健康相关数据泄露的强制性通知

30.1 控制者必须在知晓健康相关数据泄露后 72 小时内向主管监督机关和受影响者报告任何重大的健康相关数据泄露。

第十五章

健康相关数据泄露的补救权

31.1 如果数据主体因健康相关数据泄露或使用医疗算法而遭受损害，其有权获得有效补救，包括赔偿。

第十六章

保护健康相关数据泄露的举报者

32.1 任何人如果以合理理由坚信控制者或拥有健康相关数据的其他人已经、正在或打算从事可能或将要导致健康相关数据泄露的活动，则有权在受保护的情况下向独立主管机关揭发该数据泄露，并有权获得保护以免自己因在受保护的情况下揭发该数据泄露而遭到报复。

第十七章

健康相关数据泄露的责任

33.1 各会员国在确定健康相关数据泄露的责任时，应考虑以下原则：

(a) 不应(包括根据侵权行为法)不合理地限制对数据主体应负的责任，以确保数据主体可以向责任实体提出赔偿要求；

(b) 在通过有关责任的立法(包括任何管理医疗算法的立法)之前，应征求患者和卫生工作者代表的意见；

(c) 医疗算法应该被用作“推荐”工具。卫生工作者及其组织仍然为使用这些工具作出的决策向数据主体负责。

第十八章

人工智能、算法透明度和大数据

34.1 医疗算法应得到透明、公平和可预测的监管，以便：

(a) (向所有群体)提供高标准的质量、公平性和安全性；

(b) 让研究人员、软件工程师、设计师、卫生工作者和医院凭借其确定性来开发技术。

34.2 不得为了促进算法、大数据或人工智能的部署或开发而降低必须对所有治疗效果进行监测的要求。其效果尚未得到透明证明的数据处理形式应遵守本建议书的科研规定。

34.3 所有算法和人工智能都应便于监测不利影响，包括受适用的法律和联合国公约保护的特征。此规定不能用于请求、要求或记录额外的人口数据。

34.4 必须设计、实施流程和系统以发现和解决算法偏见。任何偏见都必须向数据主体披露，并由卫生工作者使用算法工具加以考虑。

34.5 使用算法、数据或人工智能作出的任何决定都应根据现有的法治要求加以解释，符合欧洲委员会下属的威尼斯委员会的法治核对表。如果某一算法不可充分解释，则只能用它来为某个决定提供支撑。任何依赖这种算法工具的卫生工作者都应为此决定负责。

第十九章

非医疗保健环境中的健康相关数据

35. 出于医疗保健和/或研究目的访问数据库中的健康相关数据或基因数据，将其用于识别、司法程序和/或调查

35.1 必须以明确、具体和合法目的收集基因数据，并且不得以与最初收集数据之目的不符的方式处理数据。

35.2 如果访问不具体的为了防止或侦查某犯罪行为或进行起诉而访问不具有的专门法证用途的数据库中的健康相关数据或基因数据，则该访问必须受到司法监督。只有在法律上存在必要的、相称的和充分的保障措施以保护数据主体的权利和利益时，方能提供访问该数据的权限。访问必须限于达到目的所需的数据。不得出于国家安全或预防犯罪的目的对该数据库进行一般性访问。

35.3 如果没有替代性或低侵入性手段来确定证据的产生是否与基因相关，以防止真正、紧迫的危险或对具体的刑事犯罪进行起诉，则只能由主管机关出于刑事执法目的处理基因数据，以防止、调查、发现或起诉刑事犯罪。

35.4 用于任何司法程序或调查的基因数据必须从数据主体那里收集，而不是由不具有专门的法证用途的数据库或生物库授权。只有在无法从数据主体那里收集数据的情况下，才可以根据法院命令允许访问具有医疗保健和/或研究用途的数据库中的数据。

35.5 只有在法律规定了适当的保障措施或显然符合个人最大利益的情况下，才能处理基因数据，以便在人道主义危机、大规模伤亡事件中识别个人，或协助识别失踪人员。

36. **健康相关数据和移民**

36.1 如果健康状况被用于就合法移民作出决定，并且为此目的收集了健康相关数据，则适用于该数据的收集、使用、共享和保留的条件同样适用于从该国公民那里收集的或关于该国公民的类似数据。

36.2 在涉及到难民和非法入境者的情况下，收集健康相关数据的先决条件是在确定个人身份过程中确保个人的尊严和人格完整性。

36.3 国家管辖范围内的经授权和未经授权的入境者和难民有权获得不低于该管辖区公民的最低标准的保健服务。

36.4 负责管理国际移民和难民方案的国际组织只能在数据共享的所有各方都遵守本建议书的规定的情况下共享健康相关数据。

37. **健康相关数据和由国家照料的个人**

37.1 本条适用于国家公办和民办机构。对于被剥削其健康决策权的个人，健康相关数据对其生活管理发挥着至关重要的作用。这些人有权和别人一样享受同等水平的医疗保健服务，尽管他们遭受的禁锢、拘留或监禁可能会有损他们对此类服务的选择。

37.2 这些原则适用于由国营或国有机构直接负责的个人，以及被国家转交给非国营部门经营者负责的个人。

37.3 访问这些人的健康相关数据必须遵守本建议书，并服务于该人的利益，而不是服务该国或机构所声称的利益。

38. **健康相关数据和营销**

38.1 只有在以下情况下，信息提供商和信息服务提供商才应促进基于健康相关数据的数据配置或营销：

(a) 尊重数据主体的隐私权和保密权；

(b) 数据配置和/或营销的存在和目的已得到明确传达；

(c) 已表示同意并予以记录，并且撤回同意可以像表示同意一样容易。

38.2 收集和出售健康相关数据的第三方必须尊重数据主体的隐私和保密性。为建立特定疾病或患者名单而将健康相关数据与其他可识别个人身份挂钩需经数据主体人同意。

38.3 广告平台不应允许基于健康特征或其代用参数，通过共享、其他访问、传输或复制等方式进行个人数据配置或目标锁定。

38.4 适用于其他健康相关数据处理的法律保护和保密规定，也同样适用于由移动健身设备或应用程序收集或披露的用于数据配置和营销的健康相关数据。

39. 健康相关数据和行为能力受损

39.1 对能力受损者决定权的限制应保持最低限度。能力受损者有权在其作出决定方面获得支持。

39.2 必须通过公平的程序来确定一个人的决定能力受损程度或是否缺乏决定能力。

39.3 一人可以指定另一人或实体代其作出决定。在代作决定时，对当事人权利的限制应保持最低限度且维护当事人的尊严，适当关怀和保护当事人。

第二十章

残疾人和健康相关数据

40.1 本建议书规定的权利和义务适用于所有个人，包括残疾人。不得歧视或污蔑残疾人。

40.2 不能强迫个人披露其残疾状况或与残疾有关的健康相关数据。如果获得福利或服务需要残疾事实证明，由主管机关提供残疾证明就足以确定享有权利。

40.3对残疾人的健康相关数据的访问必须符合本建议书的要求，并符合个人利益。访问残疾人健康相关数据的方式必须是残疾人可使用的方式。

第二十一章

性别、性别表达和健康相关数据

41.1 必须采取一切必要的行政和其他措施来管理健康相关数据，以确保享有能达到最高标准健康的权利，并不受基于性别、性别认同或性别表达的歧视。

41.2 必须特别注意收集和管理健康相关数据，包括有关用作性别平等标码的类别的数据。

第二十二章

交叉性和健康相关数据

42.1 医疗保健中的交叉性适用于从业人员和寻求医疗保健者。多种因素的相互作用可能对个人有利，也可能对个人不利。不管属于哪个社会群体，每个人都应该获得同等标准的医疗保健服务。

第二十三章

健康相关数据和应通报疾病

43.1 在出于公共利益之目的(如报告应通报疾病)而必须对公共卫生领域健康相关数据进行处理时，应该遵照按照第二章和第三章的规定，并采取适当的具体措施以保障个人权利和自由，防止对个人歧视。