保护艾滋病信息保密性和安全性的指南：

一次研讨会的进展

2006 年 5 月 15—17 日，瑞士，日内瓦

过度时期指南
2007 年 5 月 15 日

摘要

2006 年 5 月 15 日—17 日，在瑞士日内瓦召开了一个为期三天的研讨会，与会者包括各个领域的健康专家和社群成员，以及艾滋病感染者。研讨会的目的是起草保护艾滋病信息的保密性和安全性的指南草案，以及制定在不同国家检验指南的计划。会议既有全体会议，也有小组或者大组讨论。会议的主要结论、建议和下一步的计划如下。

E.1　对于保护数据，制定和实施保护敏感数据的措施受到三个相互关联的概念的影响。*隐私*既是一个法律的概念，也是一个伦理的概念。法律的概念指的是对一个人获得和使用个人信息的权利的法律保护，以便给保密性和安全性的实施提供总体框架。*保密性*指的是个人在存储、传输和使用时保护他们的数据的权利，以便防止在未授权的情况下信息被泄露给第三方。*安全性*是指通过一系列的技术手段解决物理的、电子的及程序的方面的问题来保护不断扩大的艾滋病服务中收集的各种信息。

E.2　公共卫生的目的是通过健康数据的收集、分析和发布来确保社群的健康，这就必须要谨慎考虑个人隐私权和保密性。指南必须考虑到相关文化因素，这些因素会影响政策，但是伦理原则应该指导有关如何且当使用和发布数据的决策。总的来说，指导原则应该基于人权原则。（第 5.1 部分）

E.3　定义健康信息的保密性和安全性原则的目的在于确保健康数据的获取和使用是为了促进全民健康，减少伤害而服务。为了实现这个目的，就需要在使得受益最大化和防止伤害之间取得平衡，因为受益会来源于数据的妥善和充分的使用，而伤害会来源于有意或者无意的不恰当的泄露可辨认个人身份的数据。恰当的政策、程序和技术手段必须在保护个人权利和保护公众权利取得平衡。

E.4　因为破坏保密性而导致的受伤害的风险程度取决于一个国家或者一个地方的偏见的程度，缺乏综合公共卫生安全网的程度，法律传统对于隐私的尊重程度，宗教因素和其他当地情况。

E.5　各国都应该有隐私和保密法律，如果没有的话，应该制定，而且隐私和保密法律的相关内容应该被所有管理数据的人的审查和知晓。

E.6　国家以及卫生保健系统的各个级别的组织应该制定有关如何收集、存储、传输和发布数据的安全性程序的书面政策。这样的政策需要在所有相关级别中被执行，员工必须必须懂得政策，并且签订同意他们将在工作中执行这些政策的同意书。还需要对新员工进行培训，

已经让所有员工了解相关程序的变更。

E.7　国家卫生保健系统中各个级别的组织以及国际组织必须指定一名保密和安全官员，该官员最终负责组织内部的所有艾滋病信息的保密性和安全性的事务。

E.8　保密性和安全性法律和程序的制定和审查应该有所有利益相关方的积极参与，包括艾滋病感染者，受到艾滋病影响的社群的成员，卫生保健专家，信息技术专家以及法律伦理专家。

E.9　资助组织应该遵循这些标准，并且有义务给予充足的资金执行这些政策，确保数据的收集和使用得到保护。资助组织还必须把维护这些标准作为资助执行伙伴或者执行机构的一个条件。

E.10　需要保护的不同类型的艾滋病信息——可辨认个人身份的，去除可以辨认个人身份的信息的，匿名的，累计数据，非个人数据。如何保护每种不同类型的信息的程序都必须要说明。

E.11　需要遵循一些组织程序以确保可辨认个人身份的数据和其他信息被安全地收集、传输、存储、使用、发放和处理（第 6.2-6.7 部分）。制定的政策和程序必须同时考虑纸质数据和电子系统。

E.12　对于电子信息系统的最大威胁往往不是来自于外部攻击，而是来自于在系统设计和执行中出现的内部问题。这些威胁归结为两类：因为系统错误，以及因为使用者错误而导致的数据无法使用。

E.13　完成这个指南的下一步计划包括：

E.13.1　完成抽样威胁分析

E.13.2　制定机构政策和程序范例

E.13.3　制定和实验自我评估计划

E.13.4　在联合国艾滋病规划署和美国总统 AIDS 救助紧急计划（PEPFAR）重点国家和 PEPFAR 执行伙伴中设计和开展调查，以确定这个指南的效用和适用性。

E.13.5　从联合国规划署和美国总统 AIDS 救助紧急计划（PEPFAR）重点国家和 PEPFAR 执行伙伴那里得到反馈，将反馈意见加入最终的指南。

E.13.6　通过在各国的实地试点使得指南生效。

E.13.7　将指南翻译成不同语言。

E.13.8　制定能力建设策略来支持各国保密性和安全性活动的执行。

1.0 目的

研讨会的目的是对于确保艾滋病相关信息保密性和安全性的一系列指南草案达成共识，这些信息被收集用于病人管理和监督，项目和艾滋病服务监督和评估，作为扩大在中低收入国家扩大艾滋病服务的一部分。研讨会还讨论了在这些国家可能的实施这些指南的方法。

2.0 背景

作为扩大在中低收入国家扩大艾滋病服务的一部分，收集各种信息，以促进病人管理和监督以及用于各种项目或服务的监督和评估已经日益受到重视。这样的数据可以持续地在不同地点跟踪个人，能够为临床管理提供纵向病人级别的信息。病人级别的信息对于监督和评估项目或者服务至关重要。这就需要建立信息系统，不论是书面存档还是电子存档，不但要确保病人保密性，并且要相对容易地获取在个体级别和集体级别的信息。实施体系必须解决系统实用性问题。比如，程序必须明确每天，每周或者每月最低的运作时间。他们还应该明确和管理数据系统可预见的风险，比如电子中断，人员缺乏或者自然灾害。

当病人级别数据被用于项目监督和评估时，指南需要解决哪类数据可以被使用，以什么形式被使用；这些数据在社会各个级别如何存储、使用和发布。在这次研讨会，5 中不同级别的数据受到特别关注。第一个级别是由非政府组织和社群小组提供的预防和治疗服务。第二个级别是在公共部门和私营部门收集的艾滋病相关信息的健康和其他机关。第三个级别是收集、存储和分析信息的国家级或次级（地区、地域、省级或州级）管理机构。第四个级别是特别指数据存储库，来自各种社会部门的信息可以得到存储和分析。第五个级别是传输给国际机构（双边或多边，资助者，基金会，研究机构）的信息。

在开发保护数据的方法的时候，既需要考虑避免各种环境威胁对于数据的物理保护，也需要考虑避免对于敏感信息的有意的或者无意地不当使用的保护。

影响对于敏感数据的保护措施的制定和实施的主要有三个相关概念，就是隐私，保密和安全。虽然相关，但是每个概念不同，所以需要制定和实施不同的措施。

*隐私*既是一个法律的概念，也是一个伦理的概念。法律的概念指的是对一个人获得和使用个人信息的权利的法律保护，以便给保密性和安全性的实施提供总体框架。隐私保护的权限取决于不同的法律法规。隐私保护给保密性和安全性的实施提供了总体框架。

*保密性*指的是个人在存储、传输和使用时保护他们的数据的权利，以便防止在未获准的情况下信息被泄露给第三方。这一点会对在病人级别信息被用于项目监督和评估之前是否要求病人知情同意有影响，或者是否假设任何使用公共服务的人同意他们的信息可以被用于监督和评估这些项目，以便促进这些项目为全民的服务。如果是后一种情况的话，需要决定在何种情况下，可以收集、存储和使用有名字的，匿名的，去除个人信息的数据。因此，保密性政策和程序的制定应该讨论如何适当地使用和发布健康信息，应该系统考虑隐私法律和规定所定义的伦理和法律问题。

*安全性*是指通过一系列的技术手段解决物理的、电子的及程序的方面的问题来保护不断扩大的艾滋病服务中收集的各种信息。虽然在不同级别的卫生保健提供中在确保保密性和安全性

时有一些共同的要求，但是不同级别也会有一些特定的安全性要求。在每个级别，对于安全性的讨论应该包括确认对于系统和数据的潜在威胁，各种对于安全性的威胁造成伤害的可能性，制定策略以管理每种威胁，成本和风险平衡分析以在消除安全性风险造成的伤害和管理风险所需的资源之间达到平衡。安全性必须既解决保护数据免于有意的或者无意地被不恰当地泄露，以及因为系统失误和使用者错误使得数据不能被使用。

2.1 物理安全

被用于临床管理而收集的暂时的和纵向的书面或者电子格式的生物医学信息，需要保证物理安全，比如数据应该存储在锁着的文件柜，锁着的屋子以及有安全系统的大楼里面。书面数据信息的传输应该用有锁的文件箱，通过传真发送（有一些另外的程序保护）或者使用组织内部（内部邮件）或者组织间（外部邮件）的邮件服务。散步在各地的电子数据系统也需要物理保护，比如广域网（WAN）需要通过购买的或者公共的域名保密和设置密码服务来获得保护。

2.2 电子安全性

2.2.1 *静止数据：*决定于数据在哪里存储，例如在健康设施级别，数据可能是有名字的或者是减弱可辨认身份的格式。后者可以是从完全匿名（即所有可辨认个人身份或者其他可辨认身份的信息都被去除，通过数据不再可能追溯到信息最初的来源）到去除部分信息的匿名（即去除了可辨认身份的信息，但是根据一个密码可以追溯到最初的来源。这个密码也许在数据存储的地方，或者在数据产生的地方，甚至是在一个可移动设备上，比如病人携带的智能卡。

访问个人电脑、笔记本电脑或者服务器都需要有密码、密钥卡（Key fob 是产生一次性密码的便携式信息终端），智能卡或者其他读取存储信息的安全措施来保障安全。数据会被存储为某种编码格式，并且包含读取限制，比如密码或者用户身份认证。存储在有很多计算机或者广泛网络连接的本地局域网和广域网上的数据需要使用安全技术，比如防火墙和路由器，对于访问数据进行限制。要根据数据的不同使用目的来确定其不同的可访问性，这就是所谓的“基于角色”的访问。

2.2.2 *数据传输：*对于电子数据，包括使用磁盘、CD-ROM、记忆棒、智能卡、PDA、电话交谈、编码电子邮件、加密的 FTP，加密的网络服务。这些情况下的安全手段包括编码以及运用 Public-Private Key Pair，虚拟专用网络（VPN）以及其他手段。

2.3 程序的安全

作为安全性要求的一部分，一个书面的安全性程序需要被制定，来确定收集、存储、传输和发布数据的方式。这些政策需要让接触数据的各个级别的人都了解。政策需要在相关级别得到执行，并且工作人员需要签署他们已经了解了这些政策，并且会在他们的工作中执行这些政策。这需要给新员工提供相关的培训，以及让所有的员工都了解相关程序的更新。数据发布政策应该对不同用途的数据发布做出规定，从向健康专家、亲属和朋友发布临床信息，到为了项目监督和评估，或者为了报告或研究发布医学记录或电子数据中的信息。

2.4 法律和伦理方面的因素

数据安全和发布政策在决定如何恰当第使用和发布信息的时候还必须考虑法律和伦理问题。这就必须回顾现有的隐私或保密法律中的相关规定，并且让所有管理数据的各级别都了解这些规定。这样的规定包括授权公共卫生权力的法律规定；对可辨认个人信息的数据的获取、使用、存储和发布做出规定的隐私法律；关于以人为研究对象的研究的法律等。虽然高收入国家的模式可以为加强法律保护提供有用的框架，指南的制定必须考虑在中低收入地区的不同情况或者没有法律适用。

公共卫生通过收集和发布健康数据确保社群健康的目的必须谨慎与保护个人隐私权相权衡。指南必须考虑到可能影响这些政策实施的相关文化因素。伦理原则应该指导有关数据恰当被使用和发布的决定。虽然对于可接受的恰当的数据使用会有不同的观点，但是在相关伦理原则的范围内考虑问题会有助于讨论。

2.5 已经发布的指南

许多国家已经发布的关于保密性和安全性的材料，比如法律和规定。研讨会与会者参考了一些背景材料，比如美国 CDC 的《艾滋病监测项目的技术指南》（Technical Guidance of HIV/AIDS Surveillance Programs）和美国国立标准技术研究所的有关保护信息的 800 系列；国际标准组织（International Standard Organization）；在卫生保健领域的非政府组织，比如北美中央癌症注册协会（North American Association of Central Cancer Registries）；同类杂志文章；信息技术提供商的文件，学术出版物，以及独立安全专家的出版物等。

已经发布的指南从法律、伦理、程序、电子、物理和数据发布等各方面对于保密性和安全性做出了阐释，也谈到了很多话题，比如防火墙设置，如何设置密码，怎样保护可移动电子设备，比如笔记本电脑，应该为员工提供什么样的培训，保护个人隐私的立法范例，如何从数码中去除可辨认身份的信息使得数据可以安全地被分析，传真机是否应该被用于传送保密信息等。这些指南许多都是来自高收入国家，还需要结合中低收入国家的情况做出调整。

研讨会之前以及中间，这些已经发布的指南被发送给各位与会者，很多情况下作者可以看到各种各样的出版物。这个过程大大地反映和汇集了既往发布的英语材料中的精华（附件 4）

3.0 目标

回顾和评论现有大多出自高收入国家的材料，将精华融入为中低收入国家改写的指南中，确保对于病人级别的信息的保密性和安全性可以在如下层面上被执行：

3.1）社区，非政府组织（NGO）
3.2）健康和其他机构
3.3）国家级及次级（地区/地域/省级/州级）级别
3.4）国家数据库
3.5）国际组织

4.0 方法

不同学科的健康专家和社群成员被要求参加两天半的研讨会。参加者包括国家项目管理者；基于国家的信息技术（IT）人员；各个领域的 IT 专家；数据的各种使用者，比如临床医生、统计员或流行病学家；伦理学家；法律专家和来自各国的艾滋病感染者（附件 1）。

在第一天的介绍性会议后（附件 2），被邀请者被分成 5 个工作组，每个工作组关注卫生保健系统中的一个级别（第 3.1-3.5 部分）。在 5 个工作组分别细致讨论并且向其他工作组做完汇报后，最后一天召开了一次全体总结大会，设定下面的计划。

5.0 艾滋病保密性和安全性原则

确定健康信息保密性和安全性原则的目的是确保健康数据被用于促进全民健康，减少危害。

要达到这样的目的需要不断地平衡如下因素：

a) 使得受益最大化——受益来源于数据妥善和充分地被利用。
b) 避免伤害，要避免因有意或无意泄露可辨认身份的数据[1]而造成的伤害。

这些潜在的受益和伤害可能影响个人、集体或机构。在纵向电子病人健康数据资源中蕴含的巨大的“健康商业财富”，以及在合并的和中间可获得数据中存在的越来越大的违反保密性的风险，促使人们制定如下的原则，在各种情况下，都会有助于告知这样的平衡。

政府的一个目标应该是确保将最好的信息用于为公众提供各种卫生保健。但是，在一些情况下，保密的个人健康数据被用于一些会对该个人造成伤害的地方，因此也需要保护这些信息。保护安全性，不让获得数据并不是一个绝对的目标；通过合法途径获得重要数据也应该得到保护。恰当的政策，程序和技术手段是使得保护个人利益和保护公众利益达到平衡。

造成伤害的风险取决于一个国家或者当地的偏见程度，综合公共卫生安全网络的缺乏程度，法律传统对于隐私的尊重程度，宗教因素以及当地的一些其他情况。

社会要想使得造成伤害的风险最小化，从而获得更多的健康受益，就必须促进和维护对于个人和他们的数据的保护。这样的保护不仅仅意味着制定原则、法律和政策，还建立在社会道德观念和价值观的改变上。而且取决于艾滋病感染者是否了解现存法律和政策，以及这些法律和政策如何实施。最后，全世界都认为尊重不论健康与否的所有人，可以使得最大限度地披露有利于公众利益的健康信息，而不造成伤害。

5.1 对于艾滋病信息保密性和安全性的指导原则

5.1.1 产生艾滋病数据的过程必须符合国际伦理和法律标准。保护隐私和保密性的基本伦理和法律标准存在于相关人权法律文件中。*隐私权*出自《世界人权宣言》的第 12 条；《公民权利和政治权利国际公约》第 17 条，《儿童权利公约》第 37 条。艾滋病相关的行动要确保艾滋病检测结果保密，保证不透露给第三方。[2]《联合国艾滋病承诺宣言》（UNGASS 2001）

---

[1] 可辨认身份的数据既指那些可直接辨认身份的数据，也指那些可间接辨认身份的数据，当两个独立数据源合在一起，可以有很高的可能性对应某个特定的个人，这种情况就是可间接辨辨认身份的数据。

[2] 联合国艾滋病规划署。《全球艾滋病流行报告》Report on the Global HIV/AIDS，2002 年 7 月，第 63 页。

指出“充分实现人人享有人权是对抗艾滋病的全球对策的一项要素”（第 16 段）。政府特别承诺将通过加强立法、规章和其他手段确保艾滋病感染者享有所有权利，包括隐私和保密。（第 58 段）。[3]

另一个重要的国际标准是联合国教科文组织发布的《世界生物伦理和人权宣言》。[4]该宣言的第 9 条，标题是“隐私和保密”，指出“一个人的隐私和他们的个人信息的保密应该受到尊重。应该最大限度地确保这些信息不被使用和泄露，除非是出于按照国际法，特别是国际人权法收集或者被认可的目的。”

不符合这些标准的数据收集不应该被纳入项目活动中。资助组织应该遵循这些标准，并且有义务提供足够的资金，使得项目可以实施这些标准，确保数据的收集和使用得到保护。资助组织还必须把维护这些标准作为一个实施伙伴或机构获得资助的必要条件。

5.1.2　组织，机构，和个人有责任尊重他们收集和存储的可辨认身份的数据的所对应的人权利。这些权利包括但限于：

a. 拒绝回答所提出的问题的权利；
b. 免费获得他们健康记录的副本的权利；
c. 获得、回顾和更正那些被检验为不正确的被确认的数据的权利；
d. 在适当的时候，自愿知情同意的权利；
e. 在没有不利后果的情况下，寻求纠正认识到的违背保密性的权利。

5.1.3　可以获得数据的组织、机构和个人有义务确保可以恰当地保护可辨认身份的信息的保密性和安全性。

a. 对保密性和安全性的保护是确保预防、治疗和关怀项目的质量所必需的。
b. 建立确保保密性和安全性的责任感和合理的措施有助于获得优优质的数据，向上汇报。
c. 保密性和安全性的保护方法应该结合社群，并且与减少对于艾滋病的偏见，包括对于高危人群的偏见的倡导相结合。

5.1.4　出于病人管理和监督目的采集的艾滋病相关信息和数据应该在技术上和物理上确保保密性。

5.1.5　被获准可以接触艾滋病相关信息的个人应该接受适当的培训，应该有责任保护保密性。

5.1.6　应该被全面调查破坏安全性和缺乏保密性的地方，并且进行适当的治理。

5.1.7　应该不断地对安全策略以及相关法律和政策进行审查和独立评估，并且在必要时进

---

[3] 联合国艾滋病规划署。Keep the Promise: Summary of the Declaration of Commitment on HIV/AIDS, United Nations General Assembly Special Session on HIV/AIDS, 25-27 June, 2001, New York, p. 13.

[4] United Nations Educational, Scientific and Cultural Organization. Universal Declaration on Bioethics and Human Rights. Adopted by acclamation on 19 October 2005 by the 33rd session of the General Conference of UNESCO.

行修改。

5.1.8　以下情况下，数据可以在组织或者机构之间分享：

a. 接收数据者会将数据运用于合法的健康目的；
b. 分享的数据的性质和数量是因为数据传输的原因临时发生，应该总是使能够成功完成某种任务所需的最小量。比如，如果完成某项任务化名记录就可以，那么就绝不要把可以辨认个人身份的信息提供出来。
c. 接收数据的组织应该和那些收集数据的组织采取同样的保密性和安全性措施，在数据被收集后就应该遵循。

5.1.9　组织和机构应该仅仅收集与完成他们声明的活动目的有关的信息。

5.1.10　组织，机构和个人有义务确保所有有关可辨认身份信息的保密性和安全性的政策和程序是公开透明，可获得的，包括今后可能使用那些日常收集的病人信息，以及死者信息。

5.1.11　那些不能充分保护可辨认身份的信息的保密性和安全性的组织，机构和个人应该承担责任，并且应该采取适当的补救措施。

5.1.12　个人性信息在未经本人同意前，不得提供给他人用于执法、移民控制，公共福利系统管理等非健康相关的用途，除非是个人或者人们正在面临迫在眉睫的严重物理伤害的威胁。

5.1.13　政策和程序的制定和实施应该让这些主要参与者都参加，在整个过程中艾滋病感染者和其他利益相关方都应该参与，并且应该纳入国家艾滋病关怀和治疗计划。

6.0　技术指南

6.1　数据类型

虽然收集、存储和使用的所有数据，作为扩大各国艾滋病服务的一部分，都有保密性和安全性要求，但是认识到数据有不同类型是很重要的，因为如果保密性被违反的话，不同数据的敏感性和对于病人的影响是有很重要的不同的。有以下几种主要的不同类型的信息：

6.1.1　*可辨认个人身份的数据*：个人级别的信息最重要的就是包含可以辨认个人身份的数据，比如姓名和地址。这些数据通常是从直接提供关怀服务的地方被收集的。他们通常由公共部门、非政府组织、私人部门或者国际组织支持的社区和健康机构来管理。在一些情况下，这些数据也会存储在地区性或者国家级的数据库中。这类数据还包括全国统一的身份号码，这就可以在跨社会部门，以及跨数据库与某个病人个体建立直接联系，比如，美国社会安全号码（social security number）。

6.1.2　*去除可辨认身份信息的匿名数据*：这类个人级别的信息被去除一些可辨认身份的数据，比如姓名、地址等。在很多情况下，这样的可辨认身份的信息会被用随机辨认码或者键值（key value）替代，如果有必要的话，可以是与某个个人卫生保健机构的某个人的病例

相联系的记录。这类的数据是由社群、健康机构、关键的统计员或者其他数据源那里获得的。他们在一个地区性或者国家级的数据库中被传输和管理。

6.1.3 *累计数据*：这类数据给予累计的个人级别的信息表示为一个指标，从社群、健康机构或者数据库中获得。这类数据通常在地区性及国际级的数据中管理。这类数据也是许多国际组织收集的类型。

6.1.4 *非个人数据*：所有级别的数据都需要有机构、地理、药物及用药情况，以及其他逻辑信息。

一些可以辨认个人身份的数据被列在框 1 中。指南中的大多数适用于这些不同的数据类型，除非特别指明。

框 1：通过一个或者几个如下数据可以辨认身份的数据列表

- 姓名
- 地址
- 完整通信地址
- 电话号码
- 传真号码
- 电子邮件地址
- 年龄和出生日期
- 性别
- 民族
- 社会安全号码，福利号码或者类似身份号码
- 职业
- 雇主信息
- 照片
- 遗传特征
- 植入信息（信用卡，银行账号等）
- 居住地的经度和纬度

6.2 组织和程序

6.2.1 在每个国家中，机构必须制定指南确保艾滋病相关信息的保密性和安全性，指南必须涵盖在该国或者该机构卫生保健系统内的所有操作层面，以及收集、存储和使用的不同类型的数据。这个政策文件必须是形成文字的，而且通过书面和电子的形式被广泛发布。政策文件必须说明出于什么目的可以收集数据，什么样的数据需要征得个人同意，以及可以接触到艾滋病数据的个人或集体的角色，以及他们可以接触的数据类型。这个政策文件应该与各国的各种利益相关方一同制定，包括艾滋病感染者。

6.2.2 这个政策文件必须也有如何对于个人和项目相关艾滋病数据的安全性操作进行常规检查，比如由独立安全检查员进行检查。这个政策文件也应该包括对于正在使用的技术的检查的要求，以确保通过使用这些新技术使得数据在被收集、存储、传输、发布或者使用时得到保护。

6.2.3 在收集和存储数据的每个地方，每个能够接触医疗记录或者保密艾滋病项目信息的员工都必须能够阅读到这个政策文件。病人也应该被告知有这份政策，并且可以阅读到这个政策文件。

6.2.4　所有获准处理数据的个人都应该有责任确保数据的保密性和安全性，并且有责任对可疑的违反安全性的情况进行汇报。

6.2.5　所有获准的员工必须阅读这个政策文件，而且必须接受恰当地维护保密性和安全性的措施的培训。一旦接受过培训，他们每年都应该签署一份保密声明，来表示他们已经了解这些政策，并且同意执行该政策。在新雇用的员工在获准接触保密艾滋病数据之前必须接受培训，而且必须签署保密声明。这必须是接触和使用保密数据的先决条件。

6.2.6　确保所有被获准的个人了解安全性政策，每个可能接触保密艾滋病数据的个人每隔一段时间都必须参加数据安全性培训。

6.2.7　卫生保健系统的每个级别的组织必须指定一个工作人员全面负责组织的艾滋病信息保密性和安全性问题。社区组织、健康机构、地区性和国家级数据库以及国际组织都必须设置这样的保密和安全官员（CSO）。CSO 的可能工作任务写在框 2 中。

框 2：保密和安全官员的大致工作任务：
1.1）明确和检查所有可应用的指南。确保提到信息保密性和安全性目标，符合组织要求，并且被纳入相关程序中；
1.2）阐明、检查和批准根据本机构或者组织情况编写的指南，并且对指南的执行负责；
1.3）测试、检查和证明信息保密和安全政策实施的有效性；
1.4）为保障保密和安全的工作提供清楚地指导以及可见性的管理支持；
1.5）争取信息保密和安全所需的各种资源；
1.6）批准任命组织内特定的人来负责信息保密和安全；
1.7）设立计划和项目来提高维护信息的保密性和安全性的意识；
1.8）确保信息保密性和安全性控制在整个组织中得到实施。

6.2.8　违反安全性或者违反保密性应该被汇报给恰当的部门，比如 CSO。当程序被违反，但是并没有导致向任何没有获准的人泄露保密数据的时候，问题可以在机构内部出问题的地方解决。但是当保密性被违反时，必须向资助组织的最高管理层汇报。每个违规应该立刻被调查，评估原因，制定补救措施，防止以后再次被违规。

6.2.9　政策必须在安全性问题上必须制定明确的奖惩措施。这包括组织内部对于因为员工的作为或者不作为而造成的违规所采取的人事政策，甚至包括解雇。对于更加严重的违规，还应该有法律制裁，特别是故意造成违规的情况。

6.2.10　员工怎样接触数据，不管是数据的收集、使用、发布或者处理，必须决定于他们所处的角色（框 3）。比如，临床员工需要获得他们机构的有关个人的全部记录，但是通常不需要得到其他机构的数据；地区总监需要获得他所辖地区的数据，但是并没有必要获得可辨认个人身份的数据，特殊情况下除外，比如对于某个违规的评估或者调查；数据分析师通常不需要获得可以辨认个人身份的数据。

6.2.11　员工操作收集、存储或者处理艾滋病相关信息的设备或者硬件的权限决定于员工的角色（框 3）

6.2.12　控制员工具备访问艾滋病相关数据的权限的系统必须是强大而且安全的，而且必须在某个员工不再担任某个职务的时候，有可以撤销其权限的程序。

6.2.13　在电子系统中必须设定用户在一段设定时间内处于不活动状态时可以暂停其使用。

6.2.14　系统所有确保保密性和安全性的部件都需要经过独立证实和检验。

6.2.15　用作识别某个员工可以使用电脑程序的密码的安全码需要使用最先进的工程标准、方法或者程序生成。

6.2.16　非工作人员访问和使用医疗记录或者艾滋病项目信息必须只有在警察确定数据是否被恰当使用和管理时可能发生。有政策说明访问、使用、发布和处理数据的规则。

框 3：基于角色访问控制

用于支持艾滋病服务的信息系统使得不同角色的人可以使用不同的功能。这些角色包括医生、护士、数据录入员、系统管理者及其他。明确每种不同角色对于系统开始工作有重要的意义，这样就可以明确每种角色不同的职责以及他们所需要的信息访问权限。这样做不但可以定义培训的需求，设置系统访问，最重要的是可以根据每种角色需求，为每种角色独立地设定访问保密数据的权限。

这个方法限制对于数据的访问权限，是一套适当设定用户权限的系统功能。这个方法可以通过定义系统内的“角色”来被使用于书面或者电子系统中，可以定义每种“角色”可以访问哪种数据，或者使用哪种功能。

很重要的，当个人用户被设定为某种特殊的角色的时候，他们登录系统必须用他们个人认证码。因此，即使一个人的访问权限由他们的“角色”决定，当着个人操作数据的时候记录用户的个人特征还是非常重要的。这需要审核以及员工管理。活动记录中的数据对于调查保密性违规有重要的意义。

可以将角色分级，就可以设定不同许可权限。比如，一个关怀机构的电子医疗记录系统可以设定“医疗员工”这样一个角色。所有具有“医疗员工”的角色的人能够看病人名单。可以设立一个“医生”的角色，只有“医生”这个角色可以看详细的医疗记录。如果一个“医生”角色被设定为“医疗员工”，那么这个医生可以被允许看病人名单，但是不能再能够看每个病人的记录了。

给予角色的访问权限必须在一个控制系统里面确定功能和数据目标，这个系统定义什么角色可以被允许使用这些功能和访问这些数据目标，以及谁有权规定不同介质的不同角色。

访问权限可以包括：
1）“浏览”，可以看存在的记录
2）“读取”，可以看数据目标的内容
3）“编辑”，可以编辑内容
4）“创建”，可以创建一个新的数据目标
5）“删除”，可以删除数据目标
6）“执行”，可以执行某项系统功能

介质 Agent 通常是个人用户，但是也可以是团体用户，或者外部程序。基于角色的访问权限控制政策需要符合当地隐私和保密性的法律和原则。总的来说，他们限制用户和角色的使用角色，他们对于功能和数据有直接和不同的需求，这些政策就是要保护这些功能和数据。分配给某个角色的权限一般满足于他们的职业功能的最低限度。被保护的信息不限于私人病人信息。累计数据和去除辨认身份的数据或者去除辨认身份的数据的匿名数据也要得到保护。切实的安全措施和协议在实施好的权限控制是很关键的。但是，好的保密性和隐私保护由用于实施访问权限参数的政策规定。

6.2.17　需要实施风险分析来评估在数据收集、存储、分析和发布过程中违反安全性的潜在安全风险，以及在发生违规的情况下决定如何恰当地避免。框 4 是对于这样的风险评估的一个例子。这解决数据传输中的风险。对于潜在风险或风险评估做了更加深入的讨论，如何处理这些问题的可能的方法将在最终的指南中的被阐述，在最终的指南中将有附录特别阐述。

6.3　可辨认个人身份的数据的收集

6.3.1　这些数据主要在社区或者健康机构中被收集。当收集这些数据的时候，决定收集和存储哪些个人数据要由病人的治疗需求，公共卫生的要求，以及项目监督和评估的需要而定。社区或者健康机构服务所收集的数据主要用于加强高质量的多次治疗和关怀以及不同机构间的转诊。用于项目监督和评估或者研究的个人数据必须根据文化传统配合法律得到个人的

同意，或者不需要病人同意而使用个人数据的依法制裁，或者两者都有。

6.3.2　可以辨认个人身份的数据只能由那些签订了保密协议的人收集。

6.3.3　保密性和安全性指南必须对于数据收集过程中的数据泄露进行保护，也需要对于数据的存储、分析和反馈阶段进行保护。例如病人和负责收集数据的人员的谈话必须在一个未获准的人不能听到个人数据的情况下进行。

6.3.4　个人数据的收集应该被控制在最小程度。

6.3.5　收集数据所采用的工具必须确保存储数据的准确性。

6.4　保密数据的存储

6.4.1　需要存储的个人信息的总量应该决定于病人需求和足够监督和评估特定项目或者常规卫生保健的要求，不必要的就不要收集了。

6.4.2　应该制定程序监督存储数据的系统的使用，以发现潜在或者实际的安全性违规。

6.4.3　应该进行威胁和灾难分析来评估那些增加无意的数据泄露或者存储数据的地点的数据毁坏的所有可能性，比如故意破坏的行为，火灾，地震，台风等。避免这些威胁和灾难的恰当的防范措施。

框 4：对数据传输中的威胁的评估

这里写一些有关编码和信息传输的基本威胁类型。这里并不是要讲关于编写密码的技术和使用的细节，而是对于书面系统和电子系统都可以使用的。这里描写的攻击只是对于传播本身而言的，并不是对于应用程序、主机、工作流或者与之相连的员工的攻击。安全性违规的后果对于数据的传输将导致：

- 错误的病人信息被写入接收数据的系统（目的地系统）
- 损失在目标系统中病人信息
- 不正确的关怀服务对病人造成可能的危害
- 对于病人身份信息的不当使用（例如泄密）
- 制造出了不存在的病人
- 对于当地卫生保健系统的滥用，比如非法获取药物或者服务
- 机构操作中断，比如电子通讯损失

1．标准偷听/数据中途截取：攻击者企图通过在数据传播过程中读取病人数据。这种攻击不太能够被侦测，因为它对于传输本身不会产生可见的影响。中途截取一个原始传播流技术上很简单。如果数据被编码，这样的攻击对于个人记录不会造成损害；但是，对于传播过程的扩展性监督可以让这样的缺陷暴露出来，因此可以让缺点被发现，这些缺点可以导致数据被解码，或者认证欺诈等。

2．病人记录更改：攻击者企图在数据传输过程中更改病人信息。当系统可以对照数据的一致性的时候，这种攻击可以侦测出来。复杂程度取决于编码和传输协议。这种攻击的实施可以从简单到复杂。

3．病人记录阻止：攻击者企图阻止病人记录的传输，从而有效阻止目的地系统接收信息。这样的攻击通过使用传输协议来侦测。这种攻击比较简单，因为基本上是通过中断传输路径来达到的。

4．病人记录插入：当没有匹配的病人转诊的时候，将一个不存在的病人记录发送到目的地系统。这种攻击的变量是一种病人记录重复攻击（record replay attack），此时一个合法的病人记录数据由一个攻击者重复发送。这种攻击能够被侦测。复杂程度取决于编码和传输协议。重复攻击要比一个新记录插入更容易被侦测。

5．病人记录请求：这种攻击假设传输协议或者工作流支持来自于目的地系统的对源系统的现存病人记录的请求。这种攻击基本上是当没有匹配病人记录时，请求一个现存的病人记录。这种攻击的变量是一种请求重复攻击（request replay attack），此时一个有效病人记录请求重复发向一个源系统。依据传输协议不同，这种攻击可以从简单到复杂。通常，一个直线重复比重新制造一个新的请求要简单。这种攻击可以被侦测。

6．认证欺诈：攻击者通过伪装成一个被授权的系统来请求和接收病人信息。这样的攻击能够被侦测。复杂程度取决于传输协议、传输路径以及总体工作流。

7．从匿名数据中重新辨认病人身份：攻击者运用统计技术来寻找用于保护或者分析的一个匿名病人记录的身份。这种攻击很难被侦测，除非在被损害方面前的公然行为。

6.4.4　包含个人医疗记录或者艾滋病项目数据的房间，不管是存储书面文件或者电子文件，都必须防止未经授权的人进去。

6.4.5　在机构中或者机构间的数据移动，不管是书面的或者可移动数据存储设备，都需要注意安全。

6.4.6　所有可移动或便携设备都需要在机构中注意安全，房间和文件柜应该上锁或者有恰当的监控。

6.4.7　固定的计算机或者其他硬件应该用锁或者警示装置来确保安全。

6.4.8　身份标签必须被用于固定的和便携式设备，这样可以知道设备的增加和总量，也可以察觉到设备的丢失。而且，有必要有一个所有固定和便携式设备的最新的总表。

6.4.9　总的来说，所有存储的数据应该被备份，通常是在不同的物理设备上面，这是为了防止存储数据的丢失和毁坏，也是为了遇到自然灾害或者其他数据丢失情况下可以恢复数据。因此，病人数据的备份政策应该确保备份的数据可以维持最初用于病人管理的数据同样的安全水平。

6.4.10　数据存储必须考虑数据系统预期使用年限中存储技术的变化。比如艾滋病治疗预计要贯穿于一个艾滋病感染者的一生，存储数据（包括备份）必须定期移动到更新的存储介质。

6.4.11　任何对于电子存储数据所作的添加、删除和更改都必须在一个单独文件或者日志上被记录。这个过程中生成的日志必须保证安全性，定期被检查，以及安全地被存储。

6.4.12　对于网络安全性的严格的和经常的评估是必须的。这包括确保使用防火墙或者其他所需的控制。所有电脑都必须更新反病毒和反入侵软件。

6.4.13　将电脑和不同网络连接前需要确保连接后能够保证网络的安全性。

6.5　数据使用

6.5.1 当数据可以被用于去除可以辨认身份的匿名信息形式时，数据应该被尽快以及尽可能被从实际的原信息中去除可以辨认个人身份的数据。

6.5.2　当可以追溯到最原始的医疗记录的键值（key value）和去除可以辨认身份的匿名数据一同被提供时，这些键值应该和那些可以辨认身份的数据同样的谨慎对待。为了降低违背保密性和安全性的风险，最好可以由最初产生这些数据的机构来保存这些键值和可以辨认个人身份的数据之间的联系，特别是在仅有一个或者几个人可以接触这些键值的社区和健康机构级别。

6.5.3　只有那些依据那些管理数据收集过程的指南被收集和存储的数据才能被分析。这应该得到个人同意或者符合法律规定。

6.5.4　所有获准访问和使用医疗记录或者艾滋病项目数据信息的员工必须个人有责任保护用来访问和使用数据的系统，以及保护信息本身。

6.5.5　那些未获准访问被保护的系统或者数据的人，比如清洁工，应该只有在被授权的人的严格监督下，或者只有在数据受到足够的安全措施保护的情况下才能被批准。

6.5.6　应该有一个书面政策规定可以访问艾滋病数据的个人的角色，以及他们的访问权限。

6.5.7　应该有一个书面政策说明处理机构包含艾滋病数据信件的程序，以及数据从一个地点转移到另一个地点的程序。

6.5.8　那些可以访问医疗记录或者艾滋病项目信息的人的工作地点必须是一个安全的地方。

6.5.9　当数据通过电子方式转移时，发送方和接受方应该运用公钥加密或者双因素认证。

6.5.10　当数据通过电子方式转移时，传输的数据需要用恰当的协议编码。可以用信息编码，受保护的时间，受保护的网络线，或者双因素认证。

6.6　信息发布

6.6.1　任何可能的时候，都应该最小程度地发布艾滋病相关数据。

6.6.2　应该制订一个书面的数据发布政策，而且定期检查。这需要确定艾滋病数据的目的和使用，规定哪些数据元素可以被发布，以及为了哪些目的而发布，必须包含对于小坟母人群的保护性规定。

6.6.3　随着对于数据分析的地理展示的绘制工具更多地被使用，数据发布政策必须特别考虑在地理展示时地址不要太确切，这样会非直接地辨认个人身份，比如在显示保密信息的时候必须使用地理遮罩技术。

6.6.4　任何超出公共卫生需要或者服务监督和评估的需要的目的提供艾滋病项目信息，必须签订一个科学协议说明目的，签订相关保密性声明，并且得到伦理委员会或者机构评审理事会（Institutional review board, IRB）的批准。

6.6.5　可辨认个人身份的数据多数情况下仅用于临床管理，而且应该只能由那些签订了相关保密协议的人发送或者接收。

6.6.6　非公共卫生目的对于艾滋病信息的访问，例如法律问题，应该仅在对于个人或者人们的物理伤害迫在眉睫的时候才能够被许可。

6.6.7　向维护其他疾病数据库或者国际卫生管理信息系统的人传送艾滋病数据，应该仅向这些组织传送，而且这样的组织有一致的安全性标准。

6.7　信息处置

6.7.1　如果要持有旧记录，他们应该被存储，以确保艾滋病信息的完全的保密性和安全性。

6.7.2　如果记录要被销毁，书面和电子记录都应该被销毁，包括所有的数据备份。

6.7.3　如果被更改的数据集从机构外被提供给卫生保健专家，在完成被授权的工作时，分析这些数据集的专家应该销毁这些数据集。各方必须书面声明说明这些数据集已经被销毁了。

6.7.4　应该制定一个书面数据存档政策。

7.0　结论和建议

7.1　为了保护数据，有三个相关的概念对于保护敏感数据的发展和实施会有影响，它们是隐私、保密性和安全性。*隐私*既是一个法律概念，也是一个伦理概念。法律的概念指的是对一个人获得和使用个人信息的权利的法律保护，以便给保密性和安全性的实施提供总体框架。隐私保护的权限取决于不同的法律法规。隐私保护给保密性和安全性的实施提供了总体框架。*保密性*指的是个人在存储、传输和使用时保护他们的数据的权利，以便防止在未获准的情况下信息被泄露给第三方。*安全性*是指通过一系列的技术手段解决物理的、电子的及程序的方面的问题来保护不断扩大的艾滋病服务中收集的各种信息。

7.2　公共卫生通过收集和发布健康数据确保社群健康的目的必须谨慎与保护个人隐私权相权衡。指南必须考虑到相关文化因素，这些因素会影响政策，但是伦理原则应该指导有关如何且当使用和发布数据的决策。总的来说，指导原则应该基于人权原则。（第 5.1 部分）

7.3　定义健康信息的保密性和安全性原则的目的在于确保健康数据的获取和使用是为了促进全民健康，减少伤害而服务。为了实现这个目的，就需要在使得受益最大化和防止伤害之间取得平衡，因为受益会来源于数据的妥善和充分的使用，而伤害会来源于有意或者无意的不恰当的泄露可辨认个人身份的数据。恰当的政策、程序和技术手段必须在保护个人权利和保护公众权利取得平衡。

7.4　因为破坏保密性而导致的受伤害的风险程度取决于一个国家或者一个地方的偏见的程度，缺乏综合公共卫生安全网的程度，法律传统对于隐私的尊重程度，宗教因素和其他当地情况。

7.5　各国都应该有隐私和保密法律，如果没有的话，应该制定，而且隐私和保密法律的相关内容应该被所有管理数据的人的审查和知晓。

7.6　国家以及卫生保健系统的各个级别的组织应该制定有关如何收集、存储、传输和发布数据的安全性程序的书面政策。这样的政策需要在所有相关级别中被执行，员工必须必须懂得政策，并且签订同意他们将在工作中执行这些政策的同意书。还需要对新员工进行培训，已经让所有员工了解相关程序的变更。

7.7　国家卫生保健系统中各个级别的组织以及国际组织必须指定一名保密和安全官员，该官员最终负责组织内部的所有艾滋病信息的保密性和安全性的事务。

7.8　保密性和安全性法律和程序的制定和审查应该有所有利益相关方的积极参与，包括艾滋病感染者，受到艾滋病影响的社群的成员，卫生保健专家，信息技术专家以及法律伦理专家。

7.9　资助组织应该遵循这些标准，并且有义务给予充足的资金执行这些政策，确保数据的收集和使用得到保护。资助组织还必须把维护这些标准作为资助执行伙伴或者执行机构的一个条件。

7.10　需要保护的不同类型的艾滋病信息——可辨认个人身份的，去除可以辨认个人身份的信息的，匿名的，累计数据，非个人数据。如何保护每种不同类型的信息的程序都必须要说明。

7.11　需要遵循一些组织程序以确保可辨认个人身份的数据和其他信息被安全地收集、传输、存储、使用、发放和处理（第 6.2-6.7 部分）。制定的政策和程序必须同时考虑纸质数据和电子系统。

7.12　对于电子信息系统的最大威胁往往不是来自于外部攻击，而是来自于在系统设计和执行中出现的内部问题。这些威胁归结为两类：因为系统错误，以及因为使用者错误而导致的数据无法使用。

8.0　完成指南的下一步计划

8.1　完成威胁分析示例
8.2　制定机构政策和程序示例
8.3　自我评估计划的制定和试验
8.4　在联合国艾滋病规划署和美国总统 AIDS 救助紧急计划（PEPFAR）的重点国家，以及 PEPFAR 的执行伙伴中设计并使用调查问卷，以确定指南的可用性和适用性。
8.5　从联合国艾滋病规划署和 PEPFAR 的执行伙伴获取对于过度时期指南的反馈，将反馈意见纳入最终指南中。
8.6　通过各国的实地检验来验证指南。
8.7　将指南翻译成多种语言。
8.8　开发能力建设的策略，支持各国的实施保密性和安全性的活动。