全球健康码管理系统设计建议书

本建议书旨在通过提出一种高效的全球健康码管理系统来提高在新型冠状病毒（或者其他上呼吸道流行性疾病）流行期间各国家和地区对于跨境流动人员的管理效率。为了达到这样的目标，我们将提出一种兼容绝大部分各国家和地区现有健康码的接口，用于实现不同国家和地区的机制不同的健康码系统之间的信息转换。与此同时，对于那些目前没有成系统的健康码的国家和地区，我们将给出若干种能够高效和我们的接口对接的健康码系统方案供其选择。

需求分析

综述

在2019年到2020年新型冠状病毒全球流行的背景下，各个国家和地区都不同程度地建立了本土的感染者接触追踪系统来监控并延缓疫病的扩散。然而，这些系统的机制和收集信息的种类都有一定的差异，难以做到直接互相兼容，这导致对跨境流动的人员的管理出现了一定的困难。为了尽快恢复原有的秩序，各国政府急需一个能够整合各个国家和地区的健康码或感染者接触追踪系统的信息的管理系统。与此同时，对于那些现在暂时还没有建立成体系的健康码的国家和地区，我们也有必要为其提供一份能够高效接入现有管理系统的健康码体系建议。

于是综上所述，该需求分析将分为两个部分进行：对现有方案的整合的需求分析和对合理的[现有健康码系统的分析]，能够高效整合进全球化管理系统的新健康码系统的需求分析[新接入国家和地区的技术选择建议]。

对现有健康码方案的整合的需求

鉴于现在已有许多国家和组织在运行和维护各自的健康码系统，如果对这些已有系统进行更改将会需要极大的工作量，为双方带来不必要的人力与物力资源消耗。因此我们的系统会尽量做到降低对原系统的影响与改变，将主要的工作方向和重心放在对现有系统的整合上，成为不同系统之间沟通的桥梁。同时，对于尚未普及健康码的国家和地区，我们会提出一些建议的健康码实现方案以供选择，这些方案会尽可能覆盖到各种不同的地区的需求，同时保证对我们的系统的最佳兼容。具体是否采取这些方案及实际的实现则由各国家和组织自行决定。

如上文所述，为了提高各个国家和地区对于疫情期间跨境人员的处理效率，我们需要实现各个国家和地区之间不同健康码体系的互通，即各体系之间信息的有效转换。在这个过程中，我们首先应该考虑的是各个国家之间的，以及我们的系统本身的兼容性。

兼容性主要需要从以下几方面考虑：

- 语言：系统需要兼容不同语言的字符，如名字，地区的字符
- 宗教：需要考虑到部分宗教的需求，例如基督教需要每周日去教堂
- 人口密度：部分地区人口密度较大，应该采用较严格的限制措施，而人口密度小的地区则可以降低限制措施以节约成本并减少对民众生活的影响
- 经济实力：如部分人可能没有能力或者不愿意使用智能手机
- 已有标准兼容：需要能够支持对现有健康码的转换
- 是否可以及时部署：考虑到疫情需要尽快控制，解决方案应做到在最短时间内部署以避免错过最佳抑制时机
- 易扩展性：因为目前对病毒的研究还在进行中，有可能将来会需要增加更多记录属性，所以要保证数据库便于扩展

在充分考虑以上这些兼容性需求之后， 就轮到了本健康码管理系统的主要功能——信息的整合与转换。

对于那些已经拥有成体系的健康码系统的国家和地区来说，健康码在运作过程中会生成一个包含了一定信息的数据库。库中的信息可能包含行动轨迹、体温信息、核酸检测结果及是否为密切接触者等等。而其中最重要，也是最决定性的信息就是每个人的流行病学身份：感染者、密切接触者或健康人。然而，当不同体系，不同机制的健康码系统需要相互交换信息时，最重要的流行病学身份这一信息并不能被无条件地直接交换。其原因有很多，其中最主要的原因是不同国家和地区对于信息的识别和管理的执行过程标准不同，无法直接相互信任。在这种情况下，就需要一个可以兼容大部分现有体系，并能有效处理不同国家和地区的健康码系统中的（或通过其他途径获得的，例如传统流行病学调查）不同种类的信息的接口。

通过对各个国家和地区的健康码体系以及流行病学调查方法的分析，我们总结出了所有在其中出现过的，被收集的信息种类（即所有可能需要该健康码管理系统处理的信息种类），列举如下。

- 身份证号码或ID
- 手机号或邮箱
- 住址
- 14天内的行动轨迹
- 是否与确诊人员密切接触过（详见“现有健康码分析”一节）

于是在建立接口时，我们必须考虑如何处理以上信息。

新健康码方案的设计的需求

在能够满足现有的，来自不同国家和地区的健康码系统的对接的管理系统初步完成并开始运行后，其也需要尽量满足其他国家和地区对于接入该系统的要求。鉴于之后加入的国家和地区一般都没有现有的成体系的健康码系统，我们希望给出一些适用于情况不同的国家和地区，行之有效，并且接入现有健康码管理系统时效率较高的健康码方案供其选择和参考。为此，我们做出了对新接入地区可能会用到的新健康码方案，需求分析如下。

流行病学方向

健康码存在的意义和本质就是帮助我们控制疫情的发展。根据研究，在没有合适措施的介入下，新冠的R0大约在3左右，这代表着每一个感染者平均可以再传染3个人。在这种条件下，4-7天后疫情的规模就会翻倍。与此同时，无论性别，年龄，所有与患者有过密切接触的人都有被感染的可能。因此，健康码系统需要判断人与人之间的接触，并在此之上结合一些客观属性数据（如是否到过染病高风险区，或是否有与患者发生密切接触的可能等）来对一个人的染病危险进行评估。这一系列操作的准确度将直接与健康码的效果挂钩。

个人信息安全方向

保证信息安全在如今的网络时代对每个人来说都是至关重要的。个人信息隐私的泄露会导致种种严重的后果。而在健康码的应用过程中，用户的个人信息会不可避免地被收集。这些信息有可能涉及到比较敏感的区域，同时有着被泄露的风险。因此，在建立健康码系统时需要评定各国人民对收集个人数据的接受程度，并以此合理的选择健康码架构。同时在日常运营和维护中需要尽可能的降低健康码系统发生数据泄露的风险。

研究方法

要达到上述目的，最直接的方法是进行大规模的问卷调查。但是受限于时间以及疫情的种种影响，我们无法做到进行一场样本量足够大、取样足够有代表性的问卷调查。因此，我们采用了一种间接的方式，即查阅并总结现有的、在世界范围内较为流行的应用及软件的隐私政策。这种方法看似只是间接调查，然而其好处却非常明显：

1. 可以直观明确的了解各国用户对隐私暴露的接受程度。对于我们研究的应用来说，如果它们的隐私政策不能满足那些对隐私保护要求最高的用户的需求，那么它们就不可能做到“流行”。
2. 避免问卷调查时因用户主观因素而产生的偏差。当我们把隐私泄露的风险及后果以问卷的形式（而不是真正使用应用程序前的近乎形式化的隐私条例的形式）直接呈现在用户面前时，我们有理由推

测用户会暂时高估这些风险，并在填写时出现一定的误差。
3. 避免一些潜在的问题。在用户隐私方面，除了用户本人的感受，还有很多其他需要考虑的因素（例如各地的法律等），而我们无法保证一一充分地考虑这些问题。因此，直接参考那些已经趋于完备的方案会是个不错的选择。

于是，依照上文中提到的标准，我们选定了Apple[1]，PayPal[2]以及Twitter[3]的用户隐私政策来进行综合分析。

现有隐私政策分析

个人信息隐私包括很多方面，诸如姓名、职业状况、住址等。我们不需要一一分析，只需要把健康码系统可能暴露的个人信息纳入考虑范围即可。根据已经完成的现有案例分析，现有健康码系统可能暴露的个人信息如下：

- 个人邮箱、手机号码
- 某段时间的行程
- 健康状况

对于Apple，PayPal和Twitter的用户来说，这些信息也同样有被暴露的风险。对此，它们的相应政策如下：

个人邮箱和手机号码

使用以上三种产品的时，用户在注册时会被要求提供自己的邮箱或电话号码作为必要的联系方式。以上三种产品的隐私条款中都提到了会妥善保管这些个人信息。

某段时间的行程

虽然不会实时记录用户位置，但以上三种产品都有途径取得用户在某些时刻的位置信息：Twitter在取得用户同意后可以获取用户的位置；PayPal在用户使用时也有途径获取用户位置；Apple的地图应用则可以更详细地得知这些信息。同样，它们也在隐私条款中提到会妥善保管这些信息。

健康状况

该信息较为特殊，只有Apple的隐私政策中提到了收集用户健康状况的相关信息：在用户填写知情同意书后，用户的健康信息将会被采集并用于科学研究。

结论

从以上的分析中，我们大概可以得出以下结论：

- 对于一般的个人信息（如邮箱等），大部分用户可以接受其在法律条款的约束下被声誉比较好的大公司采集。
- 对于更加私密的个人信息（如健康状况等），用户也可以接受其在自身同意的情况下被采集。
- 具体的技术性实现请参考个人信息保护问题

通用性及便利性方向

智能手机普及率不足

根据美国皮尤中心在2018年的调查数据，全球绝大部分国家智能手机普及率都在80%以下，若只发行智能手机可以使用的电子版健康码，这远未达到足以满足流行病学方面需求的程度。因此，全球健康码需要一个可以通用于智能手机用户与非智能手机用户的方案。
建议的解决方案：

1. 一机多码：通过“为家人申报健康码”功能，一机多码，家人结伴出行时，由有智能手机的家庭成员代无智能手机的家庭成员出示。
2. 纸质与电子健康码并行：保留健康码普及通用前的纸质登记方式，在固定站点纸上登记信息，并打印纸质二维码供出行使用。

平均硬件水平较低

据CSC Insight分析师尼尔沙哈（Neil Shah）的初步预计，美版健康码系统存在“数字鸿沟”（指不同人群拥有的信息技术差距），全球有近20亿的手机的硬件水平无法兼容美版健康码，在英国，有1/3的成年人的手机无法兼容，在印度，更是有60%-70%的人被排除在外。因此，全球健康码需要一个可以通用于不同程度硬件水平的智能手机用户的方案。

部分健康码方案申报过程过于繁琐

据外媒报道，Verily公司发行的健康码系统全部填写完成需要花费20-30分钟，从创建账户、填写 COVID 许可表、进行筛查、合格后提示进行新冠测试、通过邮件接收结果这五个步骤。被美国网友吐槽：“浪费时间，毫无用处。”全球目前有部分健康码在设计申报流程时，只考虑能否满足采集到所需信息的要求，忽略了用户对于申报便利性的需求，这违背了从便利角度出发的健康码系统的初衷。因此，全球健康码需要一个可以兼顾信息采集的完整性与用户申报的便利性的方案。

现有健康码系统的分析

现有的健康码种类繁多，机制各异。在此我们选择其中三种来研究，分别是中国式方案（集中式），谷歌&苹果的方案（分散化）和纸质码方案（低硬件要求）。将其与前文的需求分析对比。

中国式方案

功能赘述

中国推行的集中式健康码本质上是一个通过大数据建模获得持码者行经路线并以此进行风险分析的系统。并以二维码颜色的形式简单的展现一个人的染病风险。

具体机制

采集信息

1. 根据扫码点位置及手机信号位置采集用户近 14 天大概行程
2. 采集消费记录地点信息，如买药记录，火车飞机票记录等
3. 采集用户个人申报信息及所在单位自主申报信息

作出分类

1. 类别：根据所采集信息分为三类三种颜色：绿色→健康；黄色→欠佳；红色→危险
2. 分类方式：根据所在以及所经过地区防控危险等级、所经过场所是否有确诊患者同时进入以及自主申报的信息综合判断
3. 区别对待：绿码可自由出行；黄码需隔离观察 7 天，不可出行；红码需隔离 14 天或接受治疗，不可出行。

推广方式：

- 通过新闻等传媒让民众深切感受到病毒的危险增加民众对健康码申报的自主积极性，自下而上地推广健康码。
- 政府下发文件让各个场所及关口设立健康码检查站禁止没有绿色健康码的人通过，从而强制性确保每一个有过出行的人都已申报健康码且得到控制。

优势与劣势

优势

1. 管控严格有效，对病毒扩散起到了较好的控制效果。对所有数据的集中掌控与管理，对持有不同颜色健康码的人群的严格分类与对待，有效抑制了病毒扩散。
2. 推广踏实高效。近乎强制的推广方式让人手一码成为必然，由下而上的方式也更快让健康码普及。

劣势

1. 对个人信息特别是行程信息有较多的采集，大量的隐私信息集中于中央数据库，个人隐私保护上存在难度。
2. 仅凭是否进入同一场所或所在地区防控等级判断颜色过于笼统且比起美版健康码的直接判断效率较低。

谷歌&苹果方案

功能概述

一种用于接触追踪的蓝牙协议，在几乎完全确保用户隐私的前提下记录用户的密切接触史，并在收到用户的确诊报告时通知所有在一段时间内与该用户有密切接触的用户。

具体机制

获取用户接触史

每个用户的手机都会定时通过蓝牙广播一段字符串，该字符串具有随机性、唯一性并会定时改变。用户的手机中会储存一段时间内广播的字符串。同时，用户的手机还会持续开启接受功能，并记录收到的其他用户手机广播的字符串以及发送距离、持续时间等相关信息。这些信息同样会被储存下来。根据上文需求分析中的流行病学部分，蓝牙的传输距离足以确定密切接触行为是否发生。

告知用户接触风险

当有用户被确认为新冠病毒感染者时，该用户可以选择将该信息报告给服务器。服务器将获取储存在该用户设备上的最近广播过的字符串，并发送给所有用户用于和他们手机上储存的最近接收到的字符串对比。如果发现有相同的字符串，则说明发生过密切接触，此时程序就会发出提示警告用户。

隐私保护

由于所有发送的字符串都是随机生成并且频繁改变的，所以通过字符串来获取用户个人信息或者追踪用户的难度极高。当用户确诊时，用户确诊这一信息需要用户本人同意才会上传至服务器；同时字符串的随机性使得任何人都无法得知该用户的真实身份。在使用过程中，用户还可以可以随时选择关闭该服务。

推广方式

苹果和谷歌计划将相关应用发布在Google play 商店和 app store 中，然而截至目前（7.12），上述应用市场中并无相关应用上架。

苹果和谷歌的进一步是将该接触追踪功能置入手机操作系统层面，进而实现在iOS和安卓系统更新时自动实现接触追踪。

优缺点分析

该种方案运用蓝牙的特性来模拟疾病传播的过程，实现了高隐私度的风险评定。但是对于被判定为易感染者的用户并无强制措施，对于疫情的防控需要用户的积极参与。

纸质码方案

相关信息

中国的纸质健康码，是为了照顾一些没有智能手机的未成年人和老人而在某些地区推行的，用纸质卡片代替动态二维码的替代方案。暂时有两种纸质健康码，都需要个人到社区中心进行办理。①生成一个有效期为14天的长期健康码，如需确认最新状况，可以扫描长期健康码来获取信息。②一张记录了姓名，电话，身份证号，家庭住址的卡片，可以作为通行证使用。

优缺点分析

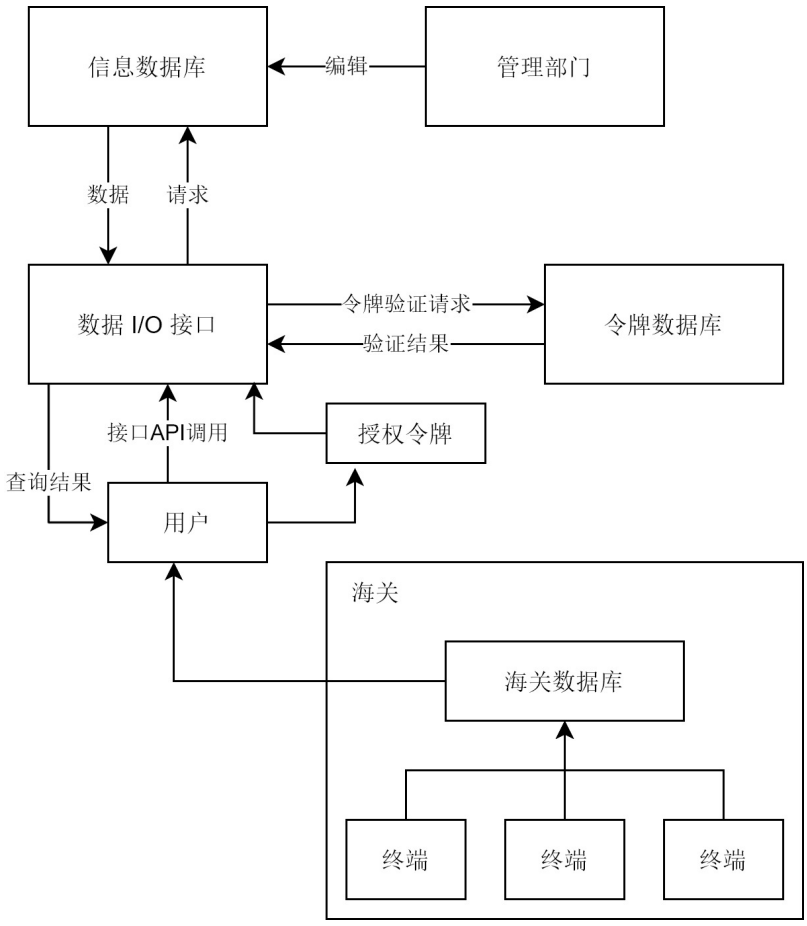
①该种纸质健康码本质上仍然需要建立在一个已成型的集中式健康码上，对于硬件和成本的要求依旧很高，只能作为对无智能手机个体的一种特殊照顾和对集中式健康码的补充存在。

②纸质健康码的媒介是纸张，信息完全手写。这导致纸质健康码有着相对低的效率，同时无法严格保证一码一人，而着信息造假的可能。但相比其他健康码，有着低成本，低要求的优点。

现有健康码系统的整合方式

标准接口：
我方标准需要成为所有现行标准的超集。在做标准转换时，现行标准属性数量应少于数据库已有数据属性数量，未填充属性则按照最差情况填写。比如，是否为密切接触者这一属性留空时，填写默认值为是密切接触者。

系统结构图：



来自用户的请求可以是读/写请求

读写请求可以分为不同的授权级别，例如：

- 级别0：只能看到密码持有人是否可以安全通过
- 级别1：只能看到有限的字段
- 级别……：
- 级别n：可以查看所有数据
- 确切的授权级别标准将在以后确定
- 不同授权等级应注明哪些值可读，哪些值可写，读写权限应进行分离

授权令牌应包括令牌持有者的详细信息：

- 注册人/公司识别码
- 授权级别
- 注册时间
- 有效期至

令牌应为

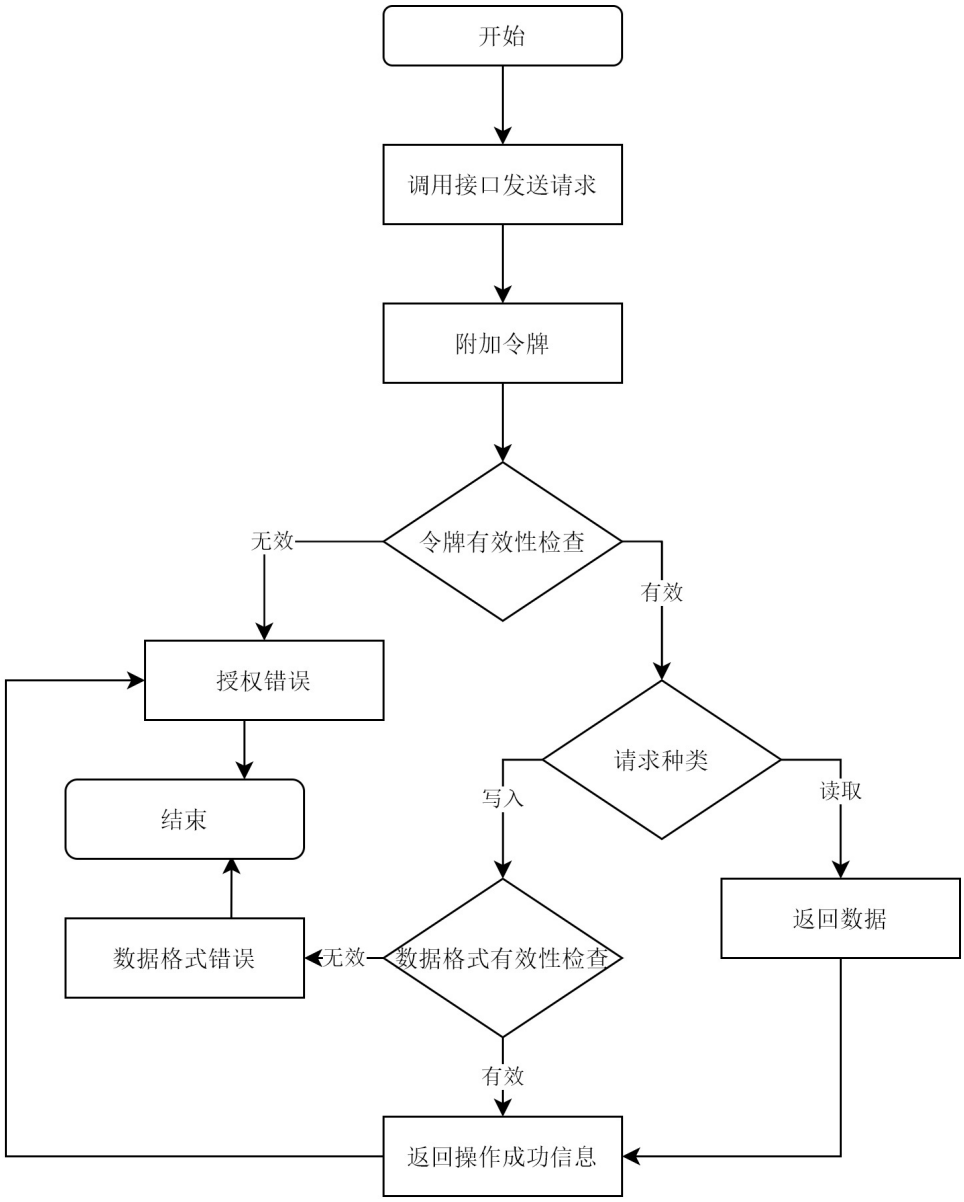
- 包含以上信息的文件
- 加密，因此令牌保留无法修改内容
- 由授权的代币分发组织分发，这些组织应由世卫组织监督和管理

所有数据流都应通过数据I / O接口[4]

所有数据库编辑都应通过管理界面[2]

用户[5]是数据请求源的统一表示，包括个人公民，政府，海关，公司等。

标准数据请求应遵循以下流程图：



总体而言，以上仅仅是大体框架上的建议，各国家内部的具体实现应结合各自的情况由自己分别决定。

新接入国家和地区的技术选择建议

对于新接入国家和地区的健康码方案，有两个基本要求。第一，符合当地情况，没有太大的推广上的障碍；第二，收集的信息能满足上文整合部分的最小信息。于是，针对情况不同的国家和地区，我们设计了不同的方案。

可供接入的方案的建议及其特点分析

集中式方案

概要

对疫情防控最严格最为可靠，对硬件水平要求较低，对个人隐私侵犯程度较大

集中式健康码应该基于可以广泛且方便传播的载体，如手机app。健康码本身以及其承载的数据应当及时更新，以确保信息的真实性和时效性。健康码软件可以通过网络运营商或是其他有效渠道来对健康码持有者的位置进行追踪和记录。同时与政府机关/医疗机构进行联网，可以对用户现状进行进行多维度的评判。新患者出现时，可以通过分析健康码云端储存的信息，对可能的密切接触者进行警告，并变更健康码颜色，必要时可以通知医疗机构对持码者进行检测。集中式健康码利用大数据技术做到对疫情的监控，但是需要足够数量的电子设备来支撑运作，同时要完成多信息库的联网有一定技术难度。

政策需求

政府需要在重要的位置设立检查点（如社区出入口，商场入口，公交车，地铁站，火车站等），来对经过的民众进行检查，以确保有染病风险的人或者患者不会进入重公共场所或者逃离隔离。同时可以令医疗机构运用数据库来精准定位易感染者并安排相关检测。

技术要求

每个用户的个人信息需与手机号绑定，且需要严格1对1。如果条件允许，可以将个人信息与政府数据库进行对接和比对，以确保信息的准确。健康需要随时间重新生成，以杜绝冒用的情况。在数据收集上，可以与网络运营商达成合作，来获取用户粗略的地理位置，又或是基于线上支付的消费记录来获得用户几天内的行经路线。在可接受的范围内，精度越高越好。健康码需要搭建完善的大数据处理系统，来对可能出现的传染案例进行评估，除了上面提到的对用户的地理位置进行分析，还可以根据用户的亲缘关系来进行加权处理。

数据安全

因为集中式健康码所涉及的数据在隐私角度来看十分敏感，在构建全球健康码时，数据安全十分重要。在本地的数据如何转移到其他国家的健康码中，转换的渠道非常重要。世界卫生组织是联合国旗下的机构，为了全世界人们的健康而存在，这样的中立组织是一个很好的中间人，可以将数据交换中心建立在世卫组织中。即使如此，这样的数据仍然需要足够强力的安全团队进行防护。需要在信息安全方面有着足够大的投入。

方案分析

集中式健康码自上而下，在管理方面有着绝对的优势，利用大数据的多维分析可以较为准确地监控疫情的发展。从流行病学角度来说，是非常有效的监控方案，因为可以有效地排查出密切接触者和患者并采取措施。但是与之相对的是对于敏感信息的担忧，集中式健康码需要收集的信息对一部分人并不在可以接受的范围，他们不喜欢自己的日常生活被记录，同时担心自己被收集的数据会泄露。所以采取这种方案时需要充分的调查民意，并同时评估构建大数据系统的可行性。

分散化方案

对于分散化的方案，我们推荐直接使用已经比较成熟的苹果及谷歌公司开发的方案（详见“现有健康码系统的分析”中“苹果&谷歌方案”一节）。其有着几乎无懈可击的用户隐私保护机制，并且目前已经在美国，德国等多个国家投入使用。

效率最高，对疫情防控较为可靠，对硬件水平要求较高，对个人隐私几乎无侵犯

纸质版方案

概述

效率较低，对疫情防控不太可靠，对硬件水平几乎无要求。

纸媒健康码应由政府统一发放，同时应当确保一码一人。通过终端或者扫描二维码就可以获得该码所有者的患病危险程度。同时，每次扫码将会在云端记录扫码时的地理位置和进入的场所。由此就可以通过在公共区域设卡来对出入的人流进行统计和记录。假如有新患者出现，就可以通过云端的数据来对可能的密切接触者进行分析调查。这种方法极大程度的减少了电子产品的使用，是低成本的动态健康码替代方案。

政策要求

纸质健康码应由政府统一发放，同时持码者每隔14天需要到最近的政府网点或医疗部门进行体温检测。政府需要在重要关口设立扫码终端，以记录进入过该区域的民众，同时阻止患病风险高的人进入公共区域。由于纸质健康码有造假冒用的可能性，需要加强关于新冠肺炎的宣传和对群众的动员，提高民众参与度。

技术要求

纸质健康码需要对用户一对一的生成永久/半永久健康码，同时可以使用终端来通过二维码对应到储存在云端的个人信息。纸质健康码的数据收集完全来源于特定场所时终端对二维码的扫描，将终端所在地点和持码者的信息登记在云端。若有人感染新冠，可以从云端的数据调取该名患者出入的公共场所，同时通过患者进出场所的时间段筛查出高危人群并在云端将其属性改为易感染者。

方案分析

相较于集中式健康码，纸质健康码只保留了对个体地理位置的记录。在利用数据分析易感染者的精度上比较有限。同时，由于收集的信息少，用户在对接其他国家的健康码系统时容易被判定为易感染者。但是相对的低成本和低硬件要求使得其成为欠发达地区的绝佳选择。原则上，并不推荐有能力推行集中式或分散式健康码的国家选择纸质健康码。

对目标国家或地区的状况分析及方案选择建议

对目标国家或地区的状况分析应主要注意以下三个指标。

1. 疫情严重程度：由此决定接入方案的防控严格程度
2. 发达水平：硬件水平、软件水平，由次决定方案的硬件要求
3. 对个人隐私侵犯的接受程度：由此决定方案的信息获取度

其决定因素需遵循以下原则：

```
发达水平 > 疫情严重程度 > 对个人隐私侵犯的接受程度
```

即在方案选取时，优先考虑级别更高的决定因素，例如，一国如果对个人隐私侵犯的接受程度低，却没有足够的硬件水平，需要优先考虑硬件水平，放弃分散式而选择集中式或纸质版健康码。以下是原因分析：

由于硬件软件水平这一因素的硬性要求，无论疫情严重程度与个人隐私侵犯接受程度如何，都不可能选择超出硬件软件水平的方案；生命财产的价值应重于个人隐私，因此疫情严重程度的考虑应大于个人隐私侵犯接受程度的考虑。

个人信息保护问题

鉴于本系统收集了所有接入国家和地区的感染者信息，对于这些信息的保护及妥善使用就成为了一个巨大的挑战。跟据信息可能泄露的途径区分，我们将从两个层面上来讨论如何保护个人信息。

技术层面（数据传输、数据调用权限等）

本系统在数据访问与传输过程中，将会使用令牌系统对数据的私密性和安全性进行保护，确保只有拥有特定权限的用户可以获取数据内容，具体实现方式：
在新用户加入时，由该系统的管理组织（如国家官方卫生部门）对用户进行授权，发放令牌（token），该令牌格式为：

- 注册人/公司识别码
- 授权级别
- 注册时间
- 有效期至

令牌为该文本经过 ***SHA-256*** 哈希算法加密后生成，确保用户无法更改。该令牌一份保留在令牌数据库内，另一份发放给用户，在典型的数据查询情况下，用户应首先在网页/手机APP内输入需要查询的索引编号，并选择授权令牌文件，通过调用数据接口API将请求与令牌输入数据I/O接口，随后数据I/O接口将发送该令牌至令牌数据库，验证该令牌是否有效，如令牌失效，返回授权错误，若令牌有效，数据库将返回该令牌的授权级别。最后数据I/O接口将授权级别和请求内容发送至信息数据库并获取该授权级别能够获取的信息内容，将该信息内容发送回用户，完成查询流程。

数据传输的每个阶段都采用https协议进行加密传输，确保信息难以被拦截篡改或破解。

组织层面（对管理数据库的组织及人员的约束）

全球健康码管理系统是一个公益性，全球性的医疗服务系统。根据该系统的性质，将其交给世界卫生组织或联合国管理应该是最好的选择。

但是考虑到各国信息隐私保护的因素，数据库本身的管理与维护应由各国官方机构完成。该机构应制定一个或多个团队负责数据库的编辑与运维工作，确保服务器的可靠性及稳定性。数据的正常输入，更改与读取应与数据库管理进行分离，数据库管理系统应采用独立网络端口与服务器进行交互，具体服务器的安全性和端口服务的设计由该机构自行设计，本建议书只对数据库格式与架构进行规定，任何因数据库管理不善所带来的影响与不便由具体管理部门承担。

结束语

健康码体系已得到世界各国家及组织的充分认可与重视，作为在疫情防控方面的重要支撑基础设施，不同健康码体系之间的沟通尤为重要。本建议书首先讨论了现有的不同健康码体系的优缺点，其次对如何进行健康码标准之间的沟通提出了概念性的构想与设计，并且为尚未部署健康码体系的国家地区提供了可参考的模板，最终着重讨论了如何在信息交互中保证数据的隐私性和安全性。

参考文献：

[1] Apple https://www.apple.com/legal/privacy/en-ww/

[2] Paypal https://www.paypal.com/us/webapps/mpp/ua/privacy-full

[3] Twitter https://twitter.com/en/privacy