Get every one in the picture

INFORMATION NOTE B

Data Confidentiality and Privacy

I. Purpose

This is a non-official document, for information only, prepared by the Working group of co-organizers of the Ministerial Conference on Civil Registration and Vital Statistics in Asia and the Pacific to be held in Bangkok, 24 November to 28 November 2014. It provides additional background information to delegations attending the Regional Preparatory Meeting for the Ministerial Conference on 28 and 29 August 2014. Published in English only.

II. Background and relevance to CRVS

Recent progress in data analytics, such as open government initiative and 'big data' applications, have brought added value to empirical data collection by enabling the production and visualization of analytical summaries to inform decision making. By making data derived from civil registration more robust, comprehensive and accessible, the value of this dataset increases dramatically. In order to benefit from civil registration systems, it is important to view registration records as assets with tangible value, held in trust by the public sector. Appropriate data handling standards should be mainstreamed at all stages, from data collection to storage and dissemination. Policies and operating procedures are needed in relation to the use of mobile devices for data collection and transmission; secure storage and archiving; and warehousing, dissemination and sharing of information as well as provision of data for research purposes.

The increasing use of mobile devices for data collection and transmission, particularly in remote areas, underscores the need to apply technical standards for data security and confidentiality of personal information. Hitherto, CRVS systems have operated in formal environments such as health centres, hospitals and government registrar offices. While this provided significantly more security than remote systems, it also has inherent problems such as difficulty of access for remote and marginalized communities. The benefits of using mobile devices are significant, but must be pursued with full awareness of the particular security challenges inherent in mobile systems, such as physical device security, communication encryption and data storage and accessibility.

III. Outline of key international conventions, recommendations and/or standards

There are no relevant international conventions which govern issues of data privacy in applicable systems. In most cases, data privacy is addressed at the national level. However, there are regional agreements and technical standards related which bear consideration. In addition, the issue has been receiving progressively more attention, with model legislation and agreements raising the profile of the issue.

- United Nations. *Fundamental Principles of Official Statistics*. http://unstats.un.org/unsd/dnss/gp/FP-New-E.pdf
- European Union. (2006). *Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.*
- European Union. (2002). *Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.*
- International Telecommunication Union. (2012). *Establishment of Harmonized Policies for the ICT Market in the ACP Countries Privacy and Data Protection: Model Policy Guidelines & Legislative Texts.*
- Health Level-7 ISO/HL7 27932:2009
- The Health Insurance Portability and Accountability Act of 1996; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996

IV. Key considerations

Innovative approaches to CRVS, in particular for birth registration, have often made use of mobile technology, including SMS for data transmission. This highlights the cost-effective and useful contribution that these technologies can make. However, SMS messages can sometimes be effectively forged, making them appear to originate from another user (SMS Spoofing). CRVS systems which anticipate the use of SMS-based mobile technologies should insure that adequate encryption and business practices are in place to prevent SMS-based systems from being vulnerable to identify theft or fraud.

Software systems, particularly those purchased from proprietary developers, are often based on the legal requirements in their countries of origin. A key example of this is Health Insurance Portability and Accountability Act (HIPPA) compliance, which provides privacy protections for health-related records (US Law). Similarly, products developed in Europe are

often designed around the legal requirements of the legislation enumerated above. Countries planning to purchase systems from these markets must be aware of these regulatory requirements and understand how they will impact their own local regulatory processes.

Further, the use of purchased software packages requires that countries carefully examine issues of intellectual property rights. Proprietary software formats should be avoided in favor of open standards, which will help insure that public sector processes do not become tied to specific software vendors or systems. Likewise, it is important that governments address data and meta-data ownership in their agreements with software providers. Because both the CRVS records themselves and data generated by the system in the collection and transmission of this information have significant and tangible value, governments should ensure that they fully understand that the data held in CRVS systems is a valuable asset being held in trust by the government for the public good of the citizens. Therefore, agreements with software development companies or service providers should give due consideration to ownership rights to both meta-data and the data itself.

Because of the very detailed nature of the codeset, the use of ICD-10 at 3- or 4-digit level for mortality data recording inherently raises individual privacy issues. For example, it is important to manage the risk that the dissemination of detailed cause of death data could enable the identification of individual deaths due to sensitive or stigmatizing conditions such as suicide or HIV/AIDS. This risk is particularly acute when data are made available at subnational and local administrative levels. While recording of this data is a necessary part of public records keeping, the release of unfiltered ICD-10 codes should be carefully reviewed. Some examples at the national level illustrate this balance by providing codes of conduct related to the research and dissemination of mortality data. These principles may include:

- Use these data for health statistical reporting and analysis only.
- For sub-national geography, do not present or publish death counts of 9 or fewer or death rates based on counts of nine or fewer (in figures, graphs, maps, tables, etc.).
- Make no attempt to learn the identity of any person or establishment included in these data.
- Make no disclosure or other use of the identity of any person or establishment discovered inadvertently and advise the institution of any such discovery.[1]

V. Relevance to the Regional Action Framework

Regional Action Framework goal 3 is most relevant to data privacy considerations. This goal, which states: “Accurate, complete and timely vital statistics (including cause of death) are produced based on registration records and are disseminated” also focuses on targets which

[1] http://wonder.cdc.gov/cmf-icd10.html

are most linked to data issues. As described above, the dissemination of detailed ICD-10 codes carries inherent privacy considerations. Therefore, targets 3.C and 3.D should be given particularly consideration. Potential solutions include recording death data with the most specific and pertinent ICD-10 code, but reporting data at a higher level of aggregation with fewer details. Other measures which could ameliorate these considerations are outlined in section IV (above).

Section F "Operational procedures, practices and innovations", and Section G "Data quality, production, dissemination and use", are highly relevant to data confidentiality and privacy. For example, paragraph 50 of the Regional Action Framework outlines potential innovative technological approaches, such as mobile devices. Handset security, communications systems, and data local data retention are all issues which should be considered under this paragraph. The preservation of privacy considerations is inherently connected to the data analysis issues described in paragraphs 51-53.

VI. Links to further information

Commonwealth of Australia (AusAID) and The University of Queensland (2011). *Strengthening practice and systems in civil registration and vital statistics: A Resource Kit.* www.uq.edu.au/hishub/docs/WP_19.pdf

United Nations Economic Commission for Europe. (2007). *Principles and Guidelines for Managing Statistical Confidentiality and Microdata Access.* http://www.unece.org/fileadmin/DAM/stats/publications/Managing.statistical.confidentiality.and.microdata.access.pdf

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cyber Crime.* http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

VII. Contacts

Mr. Matthew Perkins
Economic Affairs Officer
United Nations Economic and Social Commission for Asia and the Pacific (ESCAP)
Information and Communications Technology and Disaster Risk Reduction Division
The United Nations Building
Rajadamnern Nok Avenue
Bangkok 10200, Thailand
Telephone: +66 (0)22 88 1787
Email: perkinsm@un.org