STAYING IN CONTROL OF LAB DATA IN A WORLD OF CONNECTED DIAGNOSTICS

JEFF TAKLE[2], BRAD CUNNINGHAM[1], JOHN GILES[3]
1. Lucerae Consulting, Johannesburg, South Africa.
2. Global Connectivity, SOMERVILLE, MA, United States.
3. ICT and Privacy Law, Michalsons Law, Cape Town, South Africa.

ABSTRACT BODY:

BACKGROUND: Virtually every device maker now sees the benefits of remotely monitoring instruments through the use of connectivity (e.g. 3g mobile data), and **they are racing to bring fully connected lab- and point-of-care (POC) instruments to Africa**. But, this brings up challenging questions: *Who owns the data? What data can manufacturers access? Can they see patient data and sell it?* We need to ensure that connected instruments move critical health data faster, but not at the expense of patient privacy or MOH control.

METHODS: SystemOne, USAID, and Michalsons (a South Africa privacy law practice) evaluated the critical data protection factors that need to be considered to properly govern connected diagnostics in the developing world, survey the applicable laws, and establish an initial "best practice" guideline for MOHs, donors, and NGOs to use when evaluating options. In addition to the major legal and policy regimes in 21 nations, the Data Use Agreements (DUA), Terms of Use (TOU), and privacy policies from the following organizations were evaluated:
Cepheid • Becton Dickinson • Alere • Abbott • Daktari • Connected Diagnostics Initiative • Savics • SystemOne • DHIS2 • OpenMRS • eTB Manager • DISA

RESULTS: Substantial deficiencies were noted in most cases, due more likely to oversight than predicated strategy.
- *Insufficient legal foundation*: major privacy and healthcare legal regimes were typically not referenced, e.g. European GDPR, US Privacy Shield, South African POPI Act, and in-country law
- *Missing structural requirements:* data destruction, specific timeframes, legal opt-out, remedy for disclosure, terminology
- *Insufficient remedy:* audit capability, reporting, security incident reporting
- *Insufficient specification:* user's rights with data / ways the data can (or cannot) be used, duration of the contract, ability to publish without prior consent

CONCLUSION: Vendors clearly do not have a common understanding of the requirements for protecting this patient data across 50+ developing nations. Clear minimum standards should be created and shared with MOHs and vendors. An **MOH-centric DUA or TOU** sets the rules of ownership and permitted uses for clear ownership, roles, responsibilities and a **more equitable distribution of value** created by connected devices. USAID is working towards such a solution.

systemone Boston + Johannesburg

GxAlert

aspect See what matters.

USAID FROM THE AMERICAN PEOPLE

CONTROL ID: 2531677 + CURRENT CATEGORY: Track 3: Partnerships + KEYWORDS: connected diagnostics, gxalert, data protection