Understanding the Risks that Come from Weak Vaccination Credentials

11/3/20

ALLIED IDENTITY

SICPA

ABCorp Secure since 1795

SALAMANDER™

This document contains information that represents the current views of Allied Identity, SICPA Corporation, Salamander Technologies, and ABCorp around the issues discussed at the time of publication. Because organizations must respond to changing market conditions, it should not be interpreted as a commitment on the part of any of the companies listed above, there is no guarantee of the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. ALLIED IDENTITY, SICPA CORPORATION, SALAMANDER TECHNOLOGIES, AND ABCORP MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. Other products or company names mentioned herein may be the trademarks of their respective owners.

For more information contact:

Allied Identity Corporation
291 La Cienega Blvd. Suite 107
Beverly Hills, CA 90211, USA
www.alliedIdentity.com
Phone +1 747 215 9200

SICPA
8000 Research Way
Springfield, VA 22153, USA
www.sicpa.com
Phone +1 703 389 6586

OVERVIEW

Protecting populations from infectious diseases is challenged by increased global mobility, high population densities, emerging threats and increased public expectations on government response. Leaders at local, national, and international levels are challenged to maintain a clear picture of population health, manage testing and vaccinations in response to events, and maintain protocols in support of access control and travel. Public health monitors, health service providers and policy makers need accurate, timely, actional information that still preserves individual privacy.

Current public health data management around vaccinations is characterized by individual countries and states reliance on Immunization Information Systems "IIS" databases and/or a paper-based immunization record. The International Certificate of Vaccination and Prophylaxis (ICVP) "Yellow Card," approved by the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO), is a paper-based manual recording of medical data for use in international travel. Each state or country's IIS databases are not typically available for use by outside sources and are often woefully inadequate for all the data collected. They have never been tied to traveler information or the paper-based Yellow Card. The manual Yellow Card solution places no limits on how or who records data and does not have protections to verify the accuracy or legitimacy of any of the collected data. This system has been based on trust and encounters fraud every day.

This present situation puts all nations using the current system at risk of super-spreader incidents. The WHO and CDC have not addressed this issue over the last 15 years and continue to be politically tied up in knots with the current pandemic.

PROBLEMS TODAY

The limitations in current vaccine health data management has direct impact on managing population health, delivering health services and managing access controls and travel guidelines.

Specific challenges include:

Managing Population Health Status

- Lack of visibility and sharing of testing and vaccination information across disparate healthcare systems
- Lack of data leads to no long-term measurement of efficacy and delayed reactions to outbreaks

Delivering Local Health Services

- People lack access to their own vaccination and health data, especially in the developing world
- Lack of data transparency and sharing leads to potential overvaccination incidents
- Managing fraud is integral to keeping the already costly vaccination costs under control
- Lack of visibility of health data leads to increased risk and additional remote learning, creating additional stress for educational institutions

Fraudulent Travel Documents

- Fraud of vaccination credentials is prevalent and widespread
- No means of validating vaccination credential data leads to increased risk for events and countries
- Travel documents are not bound to strong identities creating a significant gap around enforcing border control policy
- Lack of a complete vaccination management system puts entire populations at risk

MANAGING POPULATION HEALTH STATUS

Visibility Across Disparate Healthcare Systems

Vaccinations of its citizens by licensed healthcare providers (HCPs), in the U.S. as well as many other nations, is not a shareable event with public health agencies enforceable by either policy or regulation. The vaccination is treated as private healthcare data and is not typically available even in an anonymized format for population health management. As vaccinated people move from provider to provider data is not always transferred and notifications about boosters and expirations of efficacy are not usually transferred or put into effect.

In late June, White House Coronavirus Coordinator Deborah Birx admonished healthcare industry executives on a call as COVID-19 cases surged across the South and West of America.

Per the article in the Wall Street Journal, Why Hospitals Can't Handle Covid Surges: They're Flying Blind**,** "It is easier to get data from HIV clinics in Africa than U.S. hospital data, said Dr. Birx, a former ambassador for global AIDS coordination, according to people familiar with the call. Dr. Birx declined to comment through a spokesman.

"Industry executives on the call were surprised that hospitals had widely failed to report, and they volunteered to track down offenders. The administration supplied a list.

PHOTO: ERIN SCOTT/BLOOMBERG NEWS

"It was filled with mistakes. Many hospitals on it had properly submitted data, which was missing from government records. Others were closed."

No Long-term Measurement of Efficacy

With a lack of real data overlaid against a map, it is impossible to build a strong set of policies about the use of one vaccination over another.

As an example of this issue, we have experienced multiple massive delays or dips in the supply chains of Stamaril or VF Pax (yellow fever vaccinations) when there were clearly outbreaks occurring in specific regions. The current method of response is one of delayed reactions, which has killed segments of served populations. A stronger real-time view of outbreaks against population vaccinations could save lives.

DELIVERING LOCAL HEALTH SERVICES

Participant Access to their Data

In the U.S. and many other countries, people that have been vaccinated by a public health institution, such as a school program for polio, may not have access to these records. The existing state-run IIS databases in the U.S. are not all up to date with the appropriate data sets and connectivity needed for the 21st century.

This is especially true in developing nations where vaccinations are given by a wide variety of NGOs, which do not always share records back to the country. In today's world that has been shaken by COVID-19, this will soon be a glaring issue, especially for countries struggling to get their economies back on track.

Potential Over-Vaccination Incidents

When vaccinations are freely administered by either public health officials or NGOs the activity is rarely tied to an Electronic Health Record (EHR). This health transaction is often lost in the shuffle.

The Zambian Smartercare Card for Vaccinations

In developing nations around the time of the Ebola and HIV crisis, it was discovered that well-meaning NGOs would come into a village and vaccinate everybody. This was then repeated by another well-meaning NGO without any coordination or sharing of the data. The consequence was of course over-vaccinations. As a result of these issues some private foundations funded vaccination cards for children to help stop this recurring problem. The systems had good take-up in many countries, but the data was not shared back to a central registry.

Managing vaccination costs

The costs for testing and vaccination development are enormous. This can be evidenced by the size of the expenditures from U.S. Operation Warp Speed on new vaccines. The market risks for pharma vaccine development are also significant. It is important for both the health of the world and for the economic interest of Pharma's shareholders that the risks and efforts of product development be lessened by an elimination of the fraud. This should also lower the cost to the end consumer, and it would be an improvement for all stakeholders involved to have transparent, accurate, real-time data regarding testing and vaccination transactions.

The Stress on Educational Institutions

If educators and parents cannot access records of vaccinations, they may be opening up areas of risk for the institution and the students. What has become apparent in the current pandemic is that younger children are not learning via remote methods like they do in classrooms. The collegiate levels of learning are economically being affected as well. Real-time vaccination data would be very helpful in reopening schools around the world.

FRAUDULENT TRAVEL DOCUMENTS

Widespread & Pervasive Fraud

Vaccinations are expensive for everybody, and in cases where monthly income is lower than the cost of a vaccination, a counterfeit document is a frequently used option. Over the last 5 years, I have been offered counterfeit yellow cards at Kigali International Airport in Rwanda and Lagos, Nigeria.

According to the article, *Fake Yellow Fever Cards Could Cause a Worldwide Outbreak*, "The recent shortage of vaccine, in combination with the [recent yellow fever] epidemics, has created an ideal opportunity for the people who take advantage of this situation to make a dollar.

"It has stimulated the increased use of counterfeit vaccination cards."

The article further explains that cases of ICVP "Yellow Card" counterfeiting abound in local media reports.

"In December 2018, local media in Zambia reported that ICVPs were being openly sold at the Inter-City Bus Terminus in Lusaka to travelers who could not afford the cost of getting vaccinated.

"In India, an acute shortage of ICVP and corruption has created a market for the fake yellow fever cards for travelers dating back to 2013."

No Validation of Credential Data

Even if the data is accurate on today's Yellow Card there is no way to validate the authenticity of the vaccination claim. The same issue resides in checking the validity of any COVID-19 testing. The process of checking on a person's healthcare status is in opposition to the HIPPA and GDPR privacy regulations in the U.S. and Europe. These policies have been replicated by many other nations globally.

Everything is built on trust. This presents major challenges for sponsors of large religious gatherings such as the Haji or for sporting events such as the Olympics and the World Cup. The liability and risk from super spreaders are immense.

Travel Documents are Not Bound to Strong Identities

The current and proposed systems by many vendors do not bind the vaccination or test credential to a strong identity or biometric. Whereas the current yellow card is supposed to be bound to a traveler's passport this is never validated or recorded.

Currently, there is no collection of travel data around tested or vaccinated international passengers from cross-border checkpoints.

This is a significant problem when enforcing border control policy. So, for a lack of any real data, the obvious solution is to shut down a country for the protection of its citizens.

Population Risk

Most people assume honesty around testing and vaccination certificates that travelers have presented to gain access to facilities or air travel. This is a false hope based on no real data. This fragile belief could be shattered with one incident and further damage the Airline and travel industry. It is estimated that globally up to forty percent of Yellow Cards are frauded or contain some frauded information around a vaccination. As the U.S. and other countries move to a vaccination phase for COVID-19 it will become evident that a potential super spreader event looms in the near future. The accelerated rate of COVID-19 or other pathogen infections will ensure that these become very public incidents.

THE NEED FOR STRONG IDENTITY

Absolute identity of the credential holder is necessary for trust in a vaccination data system. At a minimum, the credential should be bound to a previously vetted credential such as a passport or driver's license. The authenticity of the credential should be electronically signed and validated back to the source.

STAKEHOLDER & INDUSTRY CHALLENGES

This environment has a variety of stakeholders with competing and shared goals. It is highly political and fraught with inactivity from the responsible parties.

Based on the current situation, trust in the WHO has been shattered and the inconsistent messaging from the CDC has not helped. Each country is trying to find its own path with no obvious global leadership on this issue.

The International Civil Aviation Organization (ICAO) takes its lead from the WHO and the CDC and currently has not addressed this issue independently.

Some private foundations have funded a coalition in an effort to address this issue, but the system relies on a centralized singular database of healthcare records tied through an API to mobile apps. The data architecture may have some security holes and can allow for a rogue third-party app to express that a vaccination or test has been performed with no active validation of this transaction.

The system is based on trust of the gathered information and the data is not 3rd party certified. And there is no adherence to the current infrastructure for cross border security with a usable ICAO compliant Machine-Readable Travel Document (MRTD) that are required for cross border travel in many countries. This system does not include a no or low-cost paper document record for an individual vaccination or test transaction.

Their proposed system architecture is contrary to the legislation of many countries around the world, which have rules about having their citizen's data stored in another country.

A New Solution

There is a coalition of four organizations, Allied Identity, SICPA, Salamander Technologies, and ABCorp, that has built the modular Vaxtrac Platform and standard which has a strong patented position. In addition, Vaxtrac can certify the healthcare transaction, e.g. that test or vaccination was performed by the registered healthcare provider. More information on this approach can be found on https://alliedidentity.com/resources

CONCLUSION

In different countries or states, the issues regarding accurate and usable data for vaccination tracking may be relegated to the bottom of the budget in favor over politically visible projects as many information and communications technology (ICT) projects in healthcare often are.

The approach to ask the software vendors in the healthcare industry to voluntarily supply data to a common API may not work as each vendor might view the loss of a proprietary edge or see the HIPPA or GDRP legal challenges as risks too high to move forward.

The problems outlined in this paper demand a scalable, easy to implement, end to end solution that provides validated data to all stakeholders and ensures the health of populations and economies alike without dependencies on legacy systems that may prove to be an impediment to success.

ABOUT ALLIED IDENTITY

Built on decades of experience from our senior management, Allied Identity was founded to address the rapidly accelerating need for absolute identity in new and unique ways. The company was established with a mixture of existing technologies from our roots and brands that have been licensed from OrangeHook Corporation and additional, complementary companies and services. These include identity management, featuring the hyper-secure iBis® integrated biometric and biographic data engine and the iChip® credential Operating System, plus a series of customizable mobile apps to facilitate highly scalable identity and validation deployments with our cloud SaaS business model.

The Allied Identity name reflects our principle approach, to take the best of people, ideas, and organizations and apply them to a singular focus of improving lives through absolute identity. We are both a software and hardware company that delivers our solutions across multiple computing environments with multiple technical partnerships.

Our vision is to make governments and other healthcare participants smarter by ensuring absolute identity, and by enabling transactions and data holistically and in real-time. This improves the efficiency of governments, quality of care, saves lives, and reduces costs.

ABOUT SICPA

SICPA is a trusted security provider and adviser to governments, security banks, high-security printers, and industry – providing secured identification, traceability, and authentication materials and services. Every day, governments, companies, and millions of people rely on them to protect the integrity and value of their currency, personal identity, products, and brands. They are based in Switzerland and have 33 offices worldwide.

REFERENCES

Carlson, Robert. July 29, 2019. “Fake Yellow Fever Cards Could Cause A Worldwide Outbreak.” *Vax Before Travel.*

Evans, Melanie and Berzon, Alexandra. September 30, 2020. “Why Hospitals Can’t Handle Covid Surges: They’re Flying Blind.” *Wall Street Journal*.

