Solution Brief

IBM Cúram Identity Intelligence

Who's who and who knows who? How entity analytics help social programs reduce fraud, waste and error

Watson Health™

IBM

Highlights

- Helps social program organizations take steps that could help prevent fraud from occurring in real time
- Uses watch lists to aid the user in identifying and tracking the individuals most likely to take advantage of the system
- Helps target known fraud patterns and incorporates those patterns early in the process to help avoid a "pay-and-chase" approach to fraud and error

In a 2013 forecast of government IT spending, Gartner, Inc. reported a slight decrease compared to the previous year. But there were a few areas where spending increased. Government organizations were increasing their spending on big data for improper payment systems. According to Gartner, this increase reflected a desire on the part of governments to address fraud, waste and abuse.[1] It's a problem that is costing society billions of dollars.

- In 2014, 6.7 percent of all Medicaid payments in the US were improper, which meant that Medicaid was responsible for 14 percent (USD 17.5 billion) of all improper federal payments. This was second only to Medicare, which was responsible for almost half of improper federal payments.[2]
- The Australian Government announced plans in 2016 to overhaul checks and balances in the welfare system to recoup just over AUD 2 billion of the estimated AUD 3.5 billion the Commonwealth owed in welfare debt due to fraud and overpayments.[3]
- In Canada, the Auditor General identified CAD 1.2 billion in waste, overpayments and fraud in welfare and disability support programs. About half (CAD 663 million) was due to overdue medical reassessments to determine continued eligibility while the other half (CAD 600 million) was due to overpayments because of a poor record of checking identity or legal status.[4]
- In the UK, the Department for Work and Pensions estimated that GBP 3.5 billion was overpaid due to errors and fraud in the system; 2.1 percent of the overall benefit expenditure.[5]

Massive case overload, growing populations and the expansion of day-to-day programs are challenging organizations that deliver social programs and benefits. Ongoing cuts in funding and personnel, and attacks on the integrity of social programs because of rising attempts to abuse or defraud the system clearly call for a new approach to managing services. Post-event "pay-and-chase" approaches to recouping misappropriated funds can be expensive, time-consuming, and can have low recovery rates. Prevention of fraud, error, waste and abuse can be more efficient and effective. Social program organizations need ways to improve caseload management, reduce fraudulent claims and efficiently deliver services to citizens—all in a cost-effective manner.

As overwhelming as these obstacles may seem, organizations can make great headway toward overcoming them by adopting and deploying an entity analytics (EA) solution. IBM® Cúram Identity Intelligence can help social services agencies attack fraud and error head-on. As a result, they can help deliver more sustainable outcomes while enabling programs to do more with less.

Two causes of improper payments are the inability to authenticate eligibility and the failure to use additional data sources to support the verification process.[6] Individuals committing fraud use many techniques to mask their identity. They also take measures to hide what they are doing and with whom, with the very specific intent of taking advantage of systems, garnering services and benefits that were intended for someone else, and joining with others to collectively defraud the system. These factors compel social program leaders to consider several questions:

- What would it mean if a social program organization could prevent fraud from occurring in real time?
- What if it was discovered that a significant duplication was hidden among client and citizen identifiers? What could be accomplished with a clear understanding of who is who? What might that mean to an organization's budget?
- What if it was possible to also understand who the fraudsters had relationships with in multiple degrees and with whom they had things in common—for example, whether two suspects had lived at the same address or at one time had the same phone number?
- What if colleagues and sister agencies could quickly be warned of potential threat or fraud?
- What if it was possible to use a watch list to identify and track individuals most likely to take advantage of the system—identifying them in real time before they receive services and funding?
- What if you could target known fraud patterns and incorporate the detection of these patterns at the earliest opportunity to avoid a "pay-and-chase" approach to fraud and error?

To gain an advantage, organizations need a comprehensive view of citizens across the services spectrum. Not only might the requirements for creating an integrated, horizontal and longitudinal view of citizens help organizations to reduce fraud, waste and abuse; they can also drive operational cost-efficiencies and deliver an enhanced citizen experience. By deploying EA as a core technology, organizations can gain an edge in fraud detection and make significant gains in operational efficiencies—which are key to accommodating these requirements.

Applying entity analytics to enhance investigations

Entity analytics is an incremental context accumulator for detecting like and related entities across large, sparse, and disparate data collections including both new and old data, small and big data, to perform analytics on events, people, things, transactions and relationships.[7]

IBM Cúram Identity Intelligence deploys advanced entity analytics specifically optimized to help identify unintentional errors that might lead to incorrect payments and to help recognize nefarious individuals and organizations in spite of sophisticated attempts to mask who they are, their unscrupulous relationships and what they are doing. Cúram Identity Intelligence delivers the capability for government social programs to detect relationships between individuals within large data sets. This core functionality can help social program organizations reduce time and labor for caseload management, and help rapidly identify fraudulent behavior or errors to potentially stop them before they occur.

Comparing data in real time

Using a process called incremental context accumulation, EA detects like and related entities across large, sparse and disparate collections of old and new data. Context accumulation is an ongoing process that occurs simultaneously with analytics.

Context accumulation does much more than match new and old data. New information is compared to what was known in the past—providing context—and handled accordingly in an assertion. An assertion, for example, deems that an individual is the same as another individual or is related to another individual. A key part of this process is a method called self-correcting assertion false positives. This method means a new piece of information can reverse a previous assertion and the system corrects the assertion accordingly.

For example, if two individuals have the same name, address and phone number, a system using EA could assume that these individuals are the same person and link them together. On the other hand, if the records are updated with dates of birth that are different, the system could automatically unlink the two records as referring to the same person, create two entities and relate them as a parent and child relationship.

The EA process can be broken down into the following analytical components:

- **Detecting like entities:** This ongoing process uses context accumulation to connect entities and identifies them as the same across data records.
- **Detecting related entities:** This process is similar to detecting like entities and uses data in context to determine relationships between entities.
- **Utilizing large, sparse and disparate information:** EA typically excels at analyzing these types of data. Large data sets are populated with many records—even up to billions of records. Sparse (e.g., scattered, infrequent) and disparate (e.g., different, no basis for comparison) data represents records that may not contain much information, but can be used to make an assertion. These three data types make up a valuable resource—and demonstrate why accumulating records through context is so important.
- **Comparing old and new information:** EA is designed to operate in real time, meaning information that is new is just arriving at an organization. Old information is data from legacy or stovepipe systems. Together, new and old data form the context by which new records are compared and handled accordingly.

Along with detecting like and related entities through context accumulation, EA performs analytics on them. Analytics can take many forms ranging from collusion detection, conflict detection, space-and-time detection and hangout detection. The purpose of these analytics is to help organizations make sense of their data for enhanced decision-making. If fraud detection is the goal, then the analytics are configured to alert an organization to patterns in the data that could indicate an occurrence of fraud. If an enhanced citizen experience is the goal, then making sense out of all services rendered and having a more informed view of who is who, who knows who and associated activities can help improve the ability to serve the citizen quickly and cost-effectively.

Targeting fraud and error with entity analytics

Cúram Identity Intelligence uses EA to help social program organizations identify and detect where and when fraudulent or improper payments may be occurring. Based on the user's incoming source data, Cúram Identity Intelligence detects like and related entities and performs analytics that can help social program organizations identify and reduce these errors.

Cúram Identity Intelligence offers the capability to integrate event information into the context of like and related entities. Event information may be transactions or activities performed between entities, and this complex event processing offers a high level of pattern detection. When a condition—for example, a pattern—involving transactions that may indicate fraud or an error is known to occur within the data, Cúram Identity Intelligence can be configured to alert the organization any time that pattern occurs again.

In some program environments, an inordinate amount of time and resources is spent investigating, verifying, researching and re-researching information. Activities such as making multiple phone calls, locating files and collating and compiling the information across multiple systems are carried out to detect and determine if fraud or error is occurring. Social program organizations need to answer critical queries such as "Is this person a valid new citizen in the system?" "Is the service requested valid?" "Do they qualify?" The goal is to be able to answer these types of questions more efficiently and effectively.

Entity analytics is about more than fraud

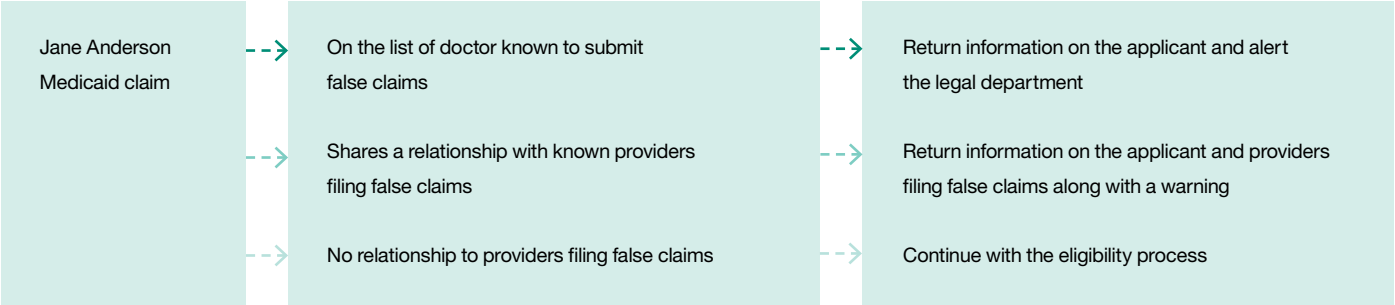
Child Welfare organizations can use Cúram Identity Intelligence to assist in conducting a background check of a foster parent applicant to assist the user as they work to determine if that individual is related to someone that may put a child at risk. For example, suppose that Johnson Smith is applying to be a foster parent. The organization receiving the application needs to know if Mr. Smith meets eligibility requirements. In a typical scenario, a caseworker doing a home study would manually search for Johnson Smith in known registries such as a child protective hotline database and would conduct background checks through local police departments. However, these manual processes take considerable time to complete and can require help from already constrained and overloaded resources. Cúram Identity Intelligence can help a caseworker to locate and review Johnson Smith's holistic dossier in a matter of seconds. Alerts and associations are presented to potentially help the user make a quicker assessment. The caseworker can view a single report, which immediately reveals that Mr. Smith has a relationship through a shared address with Frank Smith. At one time, Johnson Smith also shared a phone number with Frank Smith. However, the report shows that Frank Smith has a red alert associated with his identity. With one click, the caseworker can see that Frank Smith is identified as a known felon with a prior history of child maltreatment. Based on this investigation, the caseworker might choose not to approve Johnson Smith as a foster parent.

Helping to prevent fraud

Cúram Identity Intelligence can help social program organizations in their efforts to stop attempted fraudulent practices before they occur. For example, a Department of Health and Human Services might be pursuing a group of providers who have been caught filing false claims. The department wants to know when anyone associated with the false claim ring—such as doctors, claimants and office staff—is filing for new services from state or local agencies.

An individual named Jane Anderson files a claim for health services. How can the department determine if she is associated with the false claim ring?

Without an EA approach, this determination would be accomplished by flagging individuals manually. A claims agent would conduct a paper search to locate anyone within the ring who had already applied for services, which requires the agent to spend extra time searching across multiple systems. They may also have to make multiple phone calls to try to detect and confirm this type of activity from any of the individuals in the false claim ring.



Decision logic for preempting fraud

Using Cúram Identity Intelligence, the department can establish a watch list of individuals who need to be tracked as possible false claimants. A user interface supplies the department with the capability to define alerts and determine who and what systems need to be notified. As the service is requested, a lookup is automatically executed against the watch list, and notifications are sent to the appropriate people and systems so that they can take the appropriate actions to prevent additional fraud from occurring (see chart above).

Maintaining social program integrity

Cúram Identity Intelligence can help organizations to enhance benefits delivery and the proper use of resources. By linking clients and relationships within and among programs, it facilitates collaboration among partner organizations and can assist social program organizations in reducing overpayments or duplicate payments through appropriate matching of eligibility information. Increasing the efficiency of the intake and eligibility determination processes can help organizations speed service delivery to citizens.

High-quality entity linking can also result in more accurate data for measuring critical success factors, such as helping clients achieve self-sufficiency. Cúram Identity Intelligence can help reduce reporting and billing difficulties by supporting organizations in their efforts to reduce errors, strengthen reporting, and document client and provider compliance with the terms of participation. The solution can be integrated with other enterprise systems through a wide variety of protocols and technologies, providing a solid foundation for data management, content management, integration, data warehousing and governance. This can help organizations manage, analyze and integrate data in real time from a variety of sources, such as client databases, vendor lists, employee databases, regulatory compliance lists and streaming data feeds. Cúram Identity Intelligence helps organizations use data that originates from these sources for cross-organizational insights.

A force multiplier for the investigation team

By using Cúram Identity Intelligence, social program organizations can develop an entity-resolved repository including identities, relationship and transactions. This can provide an accurate and rich source of intelligence for an investigation team, who can access this information by using link analysis visualization tools.

About IBM Watson Health

IBM Watson Health is working to enhance, scale and accelerate human expertise across the domains of health, human services, workforce services and social security, to help people live healthier, more productive lives. It is pioneering the use of cognitive technologies that understand, reason and learn to help social program organizations unlock the potential of data and analytics to improve service delivery. To IBM, Health is not just healthcare; it is individual health, community health, employer health and economic health to help foster better outcomes at lower cost.

For more information

To learn more about IBM Cúram Identity Intelligence, please contact an IBM sales representative, or IBM Business Partner, or visit: ibm.co/socialprograms

Endtnotes

1. Gartner, Inc. "Gartner Says Worldwide Government IT Spending Flat in 2013." http://www.gartner.com/newsroom/id/2518815

2. Tara O'Neill Hayes, "Curbing Waste, Fraud, and Abuse in Medicaid." American Action Forum. March 9, 2016. https://www.americanactionforum.org/research/curbing-waste-fraud-and-abuse-in-medicaid

3. Stephen Dziedzic. "Election 2016: Crackdown on welfare payments cornerstone of Coalition's final budget costings." ABC.net. http://www.abc.net.au/news/2016-06-28/election-2016-coalition-releases-election-costings/7550790

4. Tanya Talaga. "Millions wasted in welfare programs." The Star. Dec 8, 2009. https://www.thestar.com/news/ontario/2009/12/08/millions_wasted_in_welfare_programs.html

5. Margot Huysman. "Welfare fraud and error: How much is the UK losing?" The Guardian. May 13, 2013. https://www.theguardian.com/news/datablog/2013/may/13/welfare-fraud-error-universal-credit

6. US Government. "Improper Payments Overview." Accessed October 31, 2016. https://paymentaccuracy.gov/about-improper-payments

7. http://www.ibm.com/analytics/us/en/technology/entity-analytics

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States
of America, January 2017

ZZS03279-USEN-00

Watson Health™