WHITEPAPER

Combining machine learning and rule-based artificial intelligence

HOW IMPRIVATA FAIRWARNING OPTIMIZES HEALTHCARE PATIENT PRIVACY AND DRUG DIVERSION INTELLIGENCE

imprivata®

Imprivata FairWarning Patient Privacy Intelligence and Imprivata FairWarning Drug Diversion Intelligence products employ a robust, mature combination of artificial intelligence (AI) techniques, including rule-based AI and machine learning (ML). It's important for customers to understand why using a combination of rule-based AI and machine learning techniques is critical to a successful, comprehensive monitoring solution. This whitepaper explains why your healthcare delivery organization (HDO) needs the unique approach to patient privacy and drug diversion intelligence offered with Imprivata FairWarning.

What is rule-based AI?

To understand why an HDO needs rule-based AI, it's best first to understand what rule-based AI is. Rule-based AI is an approach to building **narrow AI**, an AI system devoted to solving a specific decision problem. Rule-based AI uses a collection of if-then rules (individually termed **production rules** or **inference rules,** and collectively termed a **rule base**) to make decisions.

The "if" part of a rule (the rule's **antecedent**) is a collection of **conditions**. You can think of a condition as a declarative sentence such as "the EHR user is a physician" that may be true or false for any given EHR user or event. A rule's antecedent may contain several conditions. In principle the rule could require that just one of the conditions be true, though, more commonly, all of the conditions must be true.

The "then" part of a rule (the rule's **consequent**) is a collection of results (termed **actions**). A consequent could be a single action that adds a fact to the set of facts known about a given event. For example, an action could assert that "the user is authorized to handle prescription medications." This sort of action is typically an intermediate result. A consequent could instead combine several actions that make a final decision about how to treat an event. For example, one action could classify a given event as part of a patient privacy "chart surfing" breach, and another action could classify the breach as having moderate severity.

Here is a trivial example of a rule:

```
If
   1. The number of patients viewed by the user on a given day is
      more than three standard deviations above the mean for the
      user’s role.

   2. The user is not in the patient communications or billing
      departments.

Then
   3. Predict that the user’s events on this day contain a
      chart-surfing breach.

   4. Classify the possible breach as having moderate severity.
```

A rule base containing many such rules, together with an appropriate **rule engine** (software that decides how to apply the rules to individual cases) would presumably guide the decision whether to investigate a given set of EHR events for the possibility of a violation of a given type and severity.

How accurate can rule-based AI be?

As the above example suggests, rule-based AI can be used to make predictions rather than recommend (or automate) decisions. There are historically famous clinical production-rule systems whose outputs were deemed superior to the decisions of leading human specialists. A historically important early example was the rule-based system **MYCIN.** MYCIN produced treatment plans having an “acceptability rating” exceeding those of all Stanford Medical School faculty members with whom MYCIN was compared.[1]

MYCIN received an acceptability rating of 65% by the evaluators; the corresponding ratings for acceptability of the regimen prescribed by the five faculty specialists ranged from 42.5% to 62.5%. The system never failed to cover a treatable pathogen while demonstrating efficiency in minimizing the number of antimicrobials prescribed.

To this day, few narrow-AI applications *of any kind* can make substantially stronger accuracy claims.

If rule-based AI can be so accurate, why don't we still use it?

Rule-based systems are still widely used in enterprise business computing. Rule engines such as Red Hat Decision Manager make it easy for IT programmers to develop rich rule-based AI bespoke applications.[2] That ease of development is one reason rule-based applications remain pervasive in enterprise computing. We often fail to recognize such applications as AI because of the **AI effect**: "onlookers discount the behavior of an [AI] program by arguing that it is not *real* intelligence." Once we learn how to make a computer solve a problem well, we quickly come to think of the solution (and the method we use to produce it) as "just computing" or "just software."[3]

The right way to gauge the level of intelligence built into a software program is to apply the same standards we apply when assessing *how much intelligence a human exhibits in making the same decisions.*[4] If the software's decision quality outdoes the decision quality of human experts teaching at a leading medical school, the software is highly intelligent – regardless of the computational methods the software uses to make its decisions.

Rule-based AI is not just attractive because of its potential for high accuracy. It's also attractive because end users can easily add to a default rule base new rules that suit specific organizational needs. For example, an Imprivata FairWarning customer might add a policy that issues an alert when a general practitioner prescribes a Schedule IV narcotic, even though such physicians are legally entitled to do so. Letting end users augment ML-based AI to cover peculiar cases in this fashion is much harder to achieve, verify, and demonstrate with ML-based AI.

Finally, rule-based AI is attractive because it is the gold standard for AI decision transparency. It enjoys this status for three reasons:

1. The sequence of rules applied by a rule engine to make a specific decision constitutes a complete explanation for the decision

2. Because of the way we get the rules (a discipline termed **knowledge engineering**), the rule sequences are exactly the same justifications a human expert would provide when explaining the same decisions

3. When the rules capture administrative or regulatory policies, the fact that the AI system satisfies the policies' requirements becomes self-evident by construction

To give a deeper answer to the question, “Why did the AI make this decision?” we would have to explain the science, or administrative and regulatory policy motivations, behind the human expertise that the rule base captures. Contemporary standards of AI transparency do not expect this degree of depth in explaining AI decisions. Explaining a decision the same way a human expert would is the most we can ask for, especially when we can positively demonstrate that the decision process satisfies regulatory requirements.

If rule-based AI is so great, why does a solution need to use ML?

Like other forms of narrow AI, rule-based AI can be labor-intensive to produce and maintain, when it models highly complex human decision processes. (MYCIN contained about 500 rules.[5]) The majority of HDOs often lack the resources to develop and refine a rule base containing hundreds of bespoke rules, but a much smaller default rule base can effectively capture the essence of most common patient privacy and drug security policies, while providing complete explanations for policy-violation detection decisions driven by the rule base.

The tradeoff is that a small rule base *by itself* will either produce too many false positives, leading to what clinicians term **alarm fatigue,**[6] or produce too many false negatives, failing to achieve the AI’s practical goals. Imprivata FairWarning overcomes this limitation by combining rule-based AI with a state-of-the-art **ML alert-closing model** that filters false positives produced by the rule base.

Imprivata has developed a cutting edge, industry leading closing model. The result is a hybrid rule- and ML-based AI system that enjoys the best of both worlds:

- Complete, definitive decision explanations
- Easily demonstrable compliance with regulatory requirements
- A low false-positive rate
- High sensitivity to real policy violations

> “The right way to gauge the level of intelligence built into a software program is to apply the same standards we apply when assessing how much intelligence a human exhibits in making the same decisions.”

How does Imprivata FairWarning detect violations not captured by the rules?

Imprivata FairWarning also uses a second state-of-the-art **ML anomaly-detection and -classification model** to detect behavioral anomalies that don't fall into the common cases captured by a hybrid rule- and ML-based AI, and that are likely nevertheless to constitute policy violations. This model has already demonstrated economic benefit for many of its users. Imprivata has developed an alerting threshold that is tailored specifically toward healthcare environments. Our unique approach to anolomy detection and classification affords HDOs the ability to quickly and accurately assess and address anomalies in their environment by reducing the rate of false-positives without compromising on the accuracy of detecting true violations.

Conclusion

A healthcare-focused risk analytics requires a hybrid of rule- and ML-based AI to ensure a comprehensive, yet easy to maintain monitoring platform that yields actionable information for compliance and privacy teams. Rule-based AI is a mature, time-proven method for achieving accurate, flexible, highly transparent, and demonstrably compliant patient privacy and drug diversion intelligence. Machine learning AI supports dynamic environments with complex cases, often unmanageable by human interaction. With Imprivata FairWarning, your organization can harness the power of AI-applied analytics, contextual behavioral analytics, and dedicated expertise to improve the accuracy of your risk analytics in even the most complex environments

1. Victor L. Yu, Lawrence M. Fagan, Sharon M. Wraith, et al, "Antimicrobial Selection by a Computer: A Blinded Evaluation by Infectious Diseases Experts," JAMA (Sept. 21, 1979) Vol. 242 No. 12, pp. 1279-1282.
2. https://www.redhat.com/en/technologies/jboss-middleware/decision-manager
3. https://en.wikipedia.org/wiki/AI_effect
4. Francois Chollet, "On the Measure of Intelligence," arXiv (Nov. 5, 2019) at https://arxiv.org/abs/1911.01547 acknowledges this historical standard of intelligence while offering an interesting alternative that in our view is better suited to evaluating artificial general intelligence, which is beyond the scope of this white paper.
5. https://www.britannica.com/technology/MYCIN
6. Sue Sendelbach and Marjorie Funk, "Alarm Fatigue: A Patient Safety Concern," AACN Adv. Crit. Care (Oct.-Dec. 2013) Vol. 24 No. 4, pp. 378-386.

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com.