PBAC Platform

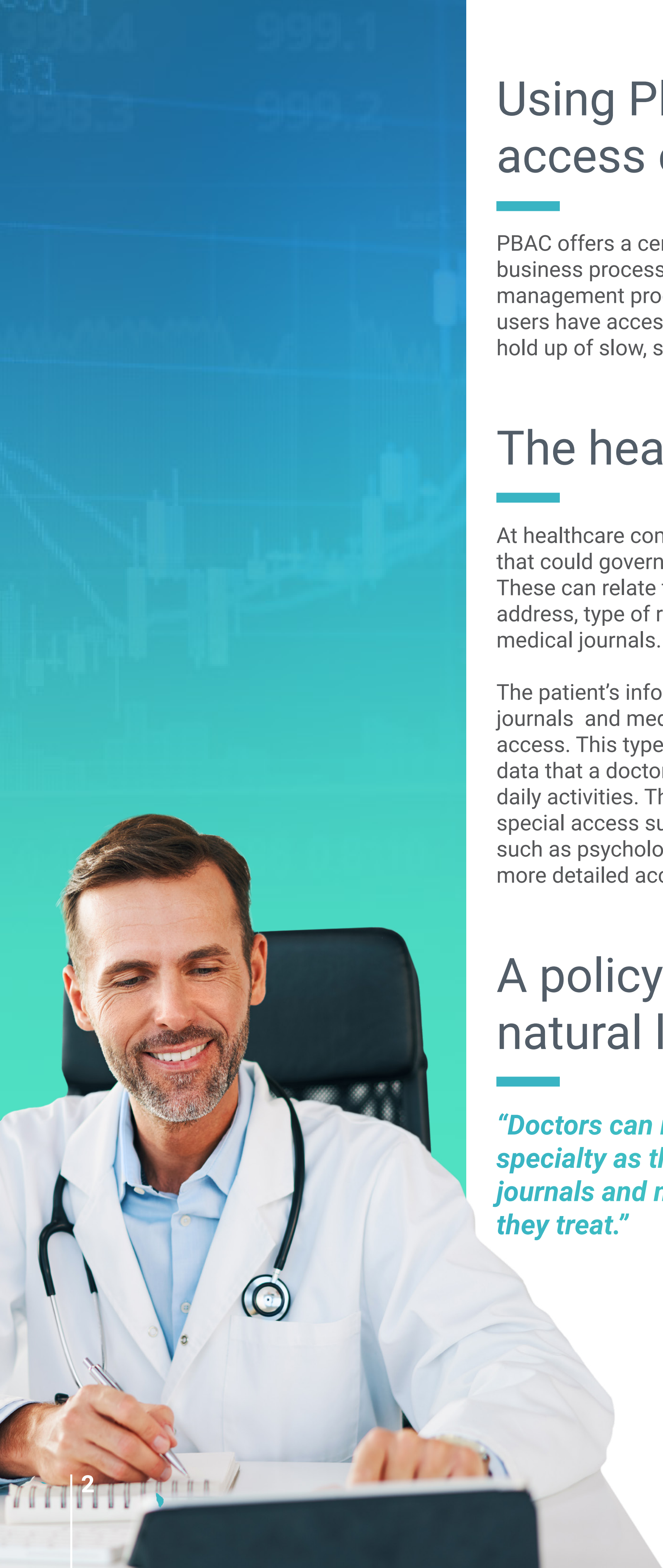
Healthcare Use Case

Introduction:

Healthcare companies handle sensitive data for a large set of clients. They operate in a highly regulated industry and need to comply with both external and internal compliance frameworks such as HIPPA, OSHA, GDPR, etc.

Healthcare companies must know exactly who has what access, but the reality is that this is a major gap in most healthcare company's security architectures.

Permissions and authorizations are often managed in siloed IT platforms and applications. Both might provision and even enforce access control. The siloed nature makes this approach cumbersome, error prone and inefficient. In order for a healthcare manager to know that a doctor or nurse has the correct access to a certain patient portal, for example, they likely need to ask the IT department, who would need to research the specific request. Many companies attempt to subvert the inefficiency by simply granting broad brush strokes of access to employees, which creates **unprecedented security risk**. Errors that stem from manual provisioning only add to this risk and create inefficiencies for the business. One of the biggest concerns is the time and money being spent by IT to administer these siloed platforms.



Using PlainID for policy based access control (PBAC):

PBAC offers a centralized approach to streamline secure business processes and to simplify back-office and IT permission management processes. This approach ensures that the right users have access to the right data at the right time without the hold up of slow, sometimes even manual, internal processes.

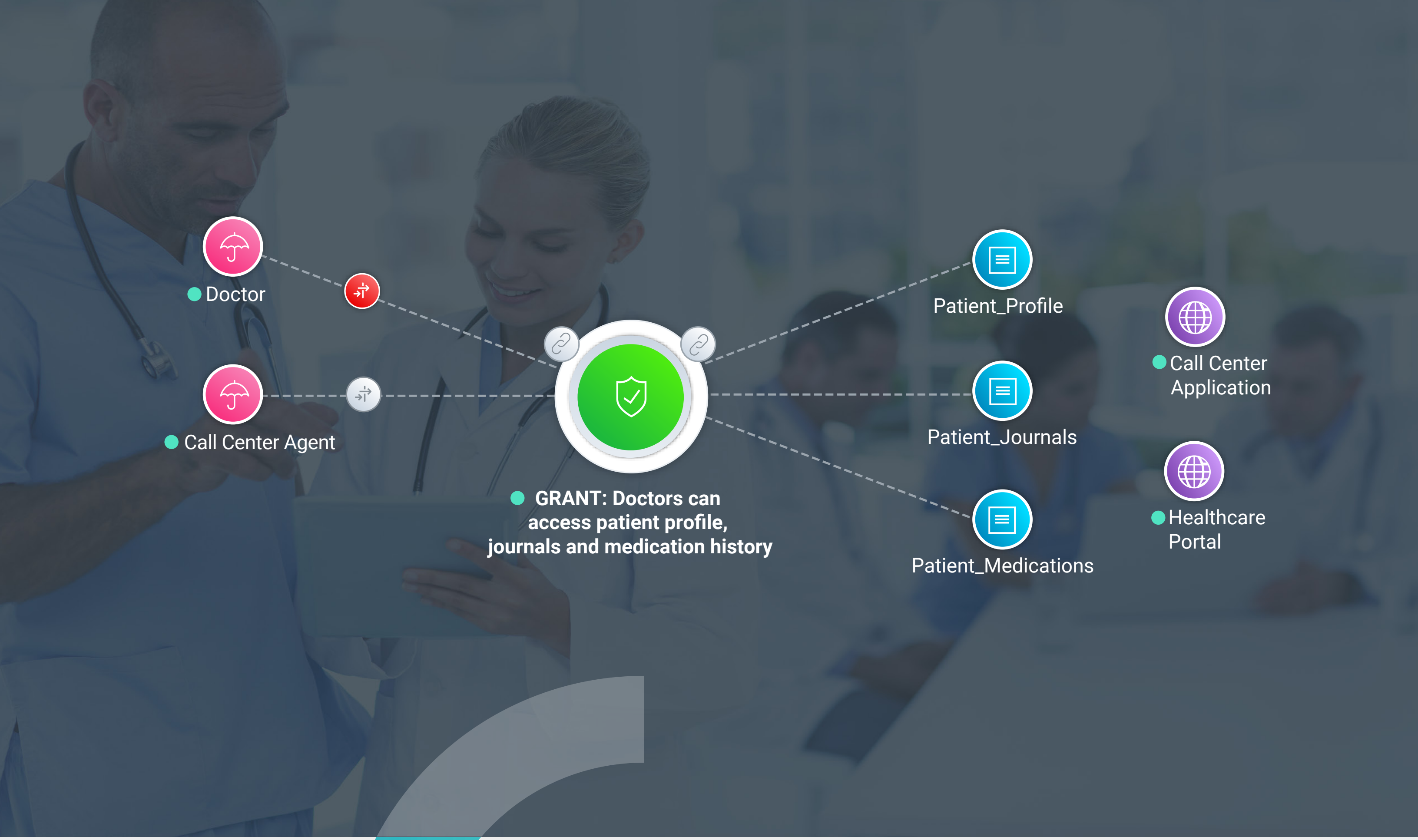
The healthcare use case:

At healthcare companies there are a multitude of business rules that could govern how client data can and should be accessed. These can relate to basic patient profile data such as home address, type of relationship with the healthcare company and medical journals.

The patient's information such as patient information, medical journals and medication records have very specific rules for access. This type of data is what we can consider basic healthcare data that a doctor or hospital staff might need to access in their daily activities. There is also other data that needs even more special access such as a restricted drugs and specific treatments such as psychological profiles where the healthcare company has more detailed access rules.

A policy example in natural language:

"Doctors can read any data of patients in the same specialty as themselves and update patient profiles, journals and medication records of patients that they treat."



How the basic policy looks in PlainID:

Note that there are no references to specific doctors in the policy. Neither are there any references to specific patient summaries, journals or medication records. The PlainID visual representation of the policy allows for a simplified and understandable view of who can access which data, down to the fine-grained layer. It also shows under which circumstances and what reasons the users are able to access the data. You can also see that one policy can govern the access control through multiple applications. On the right side of the UI, you can see two different applications, the Healthcare Portal and the Call Center Application, and both use the same policy ensuring the same user experience across multiple applications.

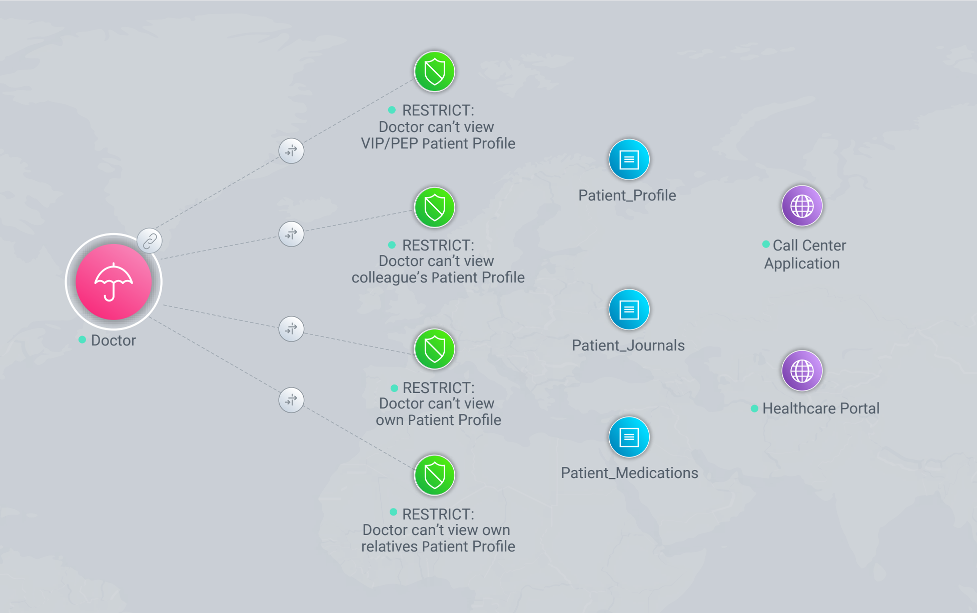
This example policy demonstrates the efficiencies and flexible access control that PBAC offers over a traditional Role Based Access Control (RBAC) model. Implementing an RBAC structure to support the policy requirements above would be nearly impossible or at least force the Healthcare Company to implement hundreds or even thousands of roles causing a massive administrative burden.

Supporting more advanced policy requirements:

Even though the basic policy above is very effective in segregating access to a healthcare company's patient data and thereby supporting basic privacy requirements aligning with the "need-to-know" principle, there are far more sophisticated privacy rules that must be incorporated. Below we have outlined some of these rules for our use case.

Restrictive access policies:

- Not access any Patient Data where the client is a "VIP"
- Not access any of my colleague's Patient Data
- Not access my own Patient data
- Not access any of my close relative's Patient Data


Doctor
RESTRICT: Doctor can't view VIP/PEP Patient Profile
RESTRICT: Doctor can't view colleague's Patient Profile
RESTRICT: Doctor can't view own Patient Profile
RESTRICT: Doctor can't view own relatives Patient Profile
Patient_Profile
Patient_Journals
Patient_Medications
Call Center Application
Healthcare Portal

The authorization decision:

At run-time when the Doctor tries to access a Patient Profile through a Healthcare Application, the application sends a simple request to the PlainID authorization rule engine.

In order for the rule engine to be able to provide an "informed decision" the authorization service needs to access the underlying healthcare data. This includes the identity data and the asset data, but also the referential data, meaning the relationships between relatives, blocked doctors and VIPs. This data could be retrieved from a variety of systems including SQL, LDAP, SCIM, REST API’s etc.

The rule engine evaluates the current user's (in this use case, the Doctor) role and also the Healthcare data to compare this data with the current Patient Profile data to be able to reach an access decision for the basic policy.

In addition, the rule engine also evaluates the restrictive rules that are part of the advanced restricted policies e.g. the Doctor’s colleagues potential blockings.

Of course, we can also use the policy decision to enable appropriate access. This approach can support access based on a "white list" or, for example, if the Doctor is assigned as a "Personal Doctor" to a patient or a set of patients.

The enforcement of access:

After evaluating all the granting access policies and the restrictive policies, the rule engine can provide an authorization decision and/or the information that Healthcare Application needs to enforce the correct access for the Doctor.

The application may use this information in-application for many purposes. Maybe it is used to provide a decision if the user needs to have access to a functional tab in the application (coarse-grained resource) or maybe the access should provide more fine-grained access due to a specific medical/health record.

The business benefit and value:

By unifying and externalizing the authorization logic from the Healthcare Application, we can now start maintaining the life-cycle of the policies in a separate process from maintaining the application logic.

The benefit of having two processes is that they now can change independently from each other. This is often very important for healthcare companies that struggle with supporting the ever-changing compliance frameworks, both internal and external.

The visibility offered through the PlainID solution ensures that no one is able to access beyond what they should, and that the business knows at all times who has access to what.

The financial benefits of PBAC include a cost reduction in application development and application maintenance efforts but also in the user management processes where PBAC provides efficiency and clarity to the business. In the longer term, significant financial and strategic benefits relate to the efforts of being able to stay compliant with regulations over time, and to be able to continuously onboard new technologies in a secure and efficient fashion. Often companies have multi-million dollar maintenance contracts that could be replaced by the capabilities of PlainID PBAC Platform.

Furthermore, the compliance control gains can decrease data breaches as well as the number of records affected by each breach. The accounting of access decisions and their enforcement is complex and voluminous. Adoption of PBAC forces an organisation to standardize the dimensions of the authorization landscape to identify and define users, roles and resources (data, applications, other). With standardized taxonomies on which to pivot access control policies the accrued benefits include not only simplification, but greater transparency around who is accessing what, when, how and why. This makes control attestation for effectiveness a much easier process in order to self-assure compliance and audit teams that information control compliance requirements are being met.