Enforcing Genetic Consent and Restrictions through a Privacy-Focused Ontology

Michael Reep, Bo Yu, Duminda Wijesekera,
Department of Computer Science
George Mason University
Fairfax, VA, USA
e-mail: mreep@gmu.edu, byu3@gmu.edu, dwijesek@gmu.edu

Paulo Costa
Dept. of Systems Engineering and Operations Research
George Mason University
Fairfax, VA, USA
e-mail: pcosta@gmu.edu

Abstract— **The use of genetic information has greatly expanded from the original focus of providing actionable data to health care providers and researchers for diagnostic and research purposes. Potential uses of this information encompass the insurance industry, employment, and law enforcement plus the more recent development of Direct-to-Consumer (DTC) tests for genealogical research. Federal and State Laws have been developed in the United States to improve privacy protections and prevent the misuse of genetic data. However, there is a wide variety of laws, regulations and restrictions governing the release criteria, level of protection required, and specificity in permitted use. The attribute-focused component of these laws matches information regarding the requester, genetic contributor with the purpose and data being released to come up with an access decision. While the attribute-based portion is easily implemented, there are numerous aspects in the laws and regulations that require more complex decision making, dictate further post-release restrictions, and specific directives for consents. A rule-base specification of these complexities can be used as a policy language to enforce data releases from electronic health records and gene pools. Our previous work developed the attribute focused aspect of the ontology along with a workflow-based prototype. The final refinements to the ontology address the more complex requirements for consent, situational validations that must be confirmed, restrictions that must be enforced after data release, actions for data protection, retention and destruction by the recipient, and informing the genetic data recipients of potential penalties for violating these restrictions. Overall this framework provides the foundation for bolstering privacy protections, enforcing the laws and regulations, and preventing the unlawful disclosures of genetic information.**

Keywords- Genetic Privacy; Electronic Medical Records; Ontology; Health Care; Genomic Medicine, Informed Consent.

I. INTRODUCTION

Numerous issues must be considered when providing comprehensive protections for genetic information. Our on-going efforts focus on providing a comprehensive framework for consistently and vigorously enforcing the laws, policies and regulations related to protecting this vital information and implementing appropriate patient consents [1]. Patients are less likely to share medical data if there is a concern about privacy, so consents are necessary to help allay these concerns [2]. Privacy concerns have been heightened as Electronic Health Records (EHRs) have become widespread and therefore most of the information are on line, so can be accessed either legally or by other means – and consequently, ensuring privacy has increased in importance [3], [4]. There are demonstrable benefits to using genetic information as genetic studies map genotypic and phenotypic data directly to diseases, allowing for preventive and early interventional care to reduce morbidity, quality of life and treatment costs [5], [6]. In addition, studies in pharmacogenomics work to use genetic information in improving the effectiveness of drugs and reduce toxicity [7]. These benefits have to be balanced against inherent unusual characteristics of genetic information that can identify a patient and his/her genetic relatives, therefore placing any of them at risk of negative consequences, such as discrimination [8], [9]. Patient concerns extend beyond the inappropriate release for insurance and law enforcement to include access within the healthcare community [10]. Consequently, laws impose penalties if genetic data is inappropriately released. Studies have also shown that de-identification of genetic material may be insufficient to protect patient privacy [11], [12].

In the United States, overall health privacy was addressed by the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which was implemented to improve the efficiency and effectiveness of the US healthcare system. HIPAA was followed by the Privacy Rule in 2000 to address three covered entities: health plans, health care clearinghouses, and certain health care providers [13]. The Genetic Information Nondiscrimination Act of 2008 (GINA) was passed to protect individuals from discrimination in employment and insurance based on genetic information [14]. Furthermore, almost every state and the District of Columbia have laws that specifically address genetic protections to some degree. However, even when patients are specifically provided information on GINA as part of pharmacogenomic testing, the subjects still report having little understanding of the act or privacy protections [15]. Health Information Exchanges and direct sharing between health care providers are still subject to the applicable state laws even for interstate data transfers [16]. This paper further develops an ontology that provides the syntactical elements (i.e., entities and their relationships) sufficient to specify applicable legislation and regulations in the forms of a machine enforceable structured rule-base.

In our previous work, we developed a prototype that uses a medical workflow system for an EHR to enforce Federal and

State laws in addition to organizational policies [17], [18]. Workflows provided the mechanism to gather the necessary information within the context of request to share genetic information in an EHR. We prepared an initial genetic privacy ontology and sample rules to enforce laws in selected states to validate our approach. We then extended the genetic privacy ontology, based directly on relevant Federal and state laws, to focus on the attribute-focused components that generate the initial access decision [18]. This paper provides further expansion and refinement of the more complex legal requirements for ensuring the appropriate consent is obtained prior to information release, validating pre-conditions for release have been addressed, and establishing the post-release protection mechanisms.

Our next step is developing this comprehensive genetic privacy ontology based directly on relevant Federal and State laws. Following this Introduction, Section II addresses related work; Section III provides an overview of the genetic privacy ontology; Section IV refines the aspects of the ontology related to consent and restriction enforcement; Section V specifies the rule base using a predicate-based authorization framework, Section VI develops an implementation example with rule definitions and an example focused on obligations, and, finally, Section VII presents conclusions.

II. Related Works

There are existing standards and frameworks with methods to implement various aspects of genetic privacy protections. Integrating the Healthcare Enterprise (IHE) standards profiling organization has developed frameworks, use cases, and specifications for managing the sharing of documents between organizations [19]. The inter-organizational policies must be completed prior to the use of this standard for implementing the consent agreements. There is some but not all the required capability to address components of genetic privacy related to acknowledging consents. For example, the use case of individuals specifying that other specific individuals do, or do not, have access to their data is listed as a scenario that is explicitly not supported [20]. Many state laws call for this type of consent specifications as a prerequisite for permissible access to data. Concepts like Dynamic Consent in biobanks provide opportunities to address the complex requirements inherent in genetic privacy [21]. Dynamic Consent engages the research participant in a real-time personalized process to obtain and update consent as needed. Dynamic Consent is also incorporated into the Bilateral Consent Framework (BCF) which use other techniques and entities such as a trusted mediator to operate the system, auditing, a code of conducts and reputation system to improve and enhance the consent process [22]. However, both Dynamic Consent and BCF have components that would require changes to state laws which often specify how and when consent must be obtained.

The restrictions placed by regulatory environments on information sharing has been identified as an issue that requires coordination across system silos [23]. The Global Alliance for Genomics and Health (GA4GH) provides a framework for sharing genome data with privacy and security policies, technology recommendations, guidance and architecture to allow interactions between organizations [24], [25]. The basis of data sharing in GA4GH is that the donors or their representatives have provided consent in accordance with organizational policies and the applicable laws [26]. The work to date provides comprehensive policies but does not have a functional mechanism for implementing sharing data or addressing the restrictions placed by donors in systems that hold and use such data. The National Institute of Health (NIH) Office of Science Policy (OSP) collaborated with GA4GH to develop a set of consents to improve consistent identification of how genomic data is used [27]. Further work was performed to reclassify these codes into a set of Categories (Primary and Secondary) and Requirements (additional agreements needed for re-use) [28]. The consent code base is focused on research with some additional restrictions than found in State Laws which could be incorporated into the ontology. These codes and NIH processes should be cross-referenced with other standards such as HL7 to provide a more complete representation.

Other health-care privacy ontologies have some overlap with genetic privacy concepts based on laws. However, these ontologies have gaps in numerous areas when compared to implementation requirements of state laws. The HL7 Security and Privacy Ontology has a class PurposeOfUseOntology with a purpose code and description [29]. Because the focus is on health care organizations, the main categories in this ontology are for health care marketing, operations, payment, research, public health and treatment with options for patient requested inquiries including family, power of attorney and support network. This list does not include key purposes regulated by law, such as Law Enforcement, Homeland Security and Insurance access. Other matching HL7 ontologies have some overlap (such as Organization, ObligationPolicy, Refrain, and Role) but not a complete set of genetic information related categories. The Sensitivity class contains a genetic disease information sensitivity but this needs to be set based on the state law attributes of the ontology. Many of the state laws have conditions that must be met prior to releasing genetic information in addition to imposing specific obligations to be adhered to after the release. The Consent component is addressed on a limited scale with options for delegation but not addressing aspects such as capacity. The ontology also has a smaller set of obligations and "refrains" to address some restrictions. A future research option is to develop a mapping and extension between our genetic focused ontology and the HL7 framework as a basis for an implementation.

Genetic privacy protections issues are expanding with the introduction of big data repositories and Direct-to-Consumer (DTC) DNA testing [30]. Adoption of the latter has skyrocketed with its lower prices and wide-spread advertising. DTC DNA testing-related sites encourage sharing of genetic data, including through the use of social media. Naveed et al. provide a Genomic Data Handling Framework to track the protections required from initial collection through to storage and use. The framework groups the uses into the general categories of Healthcare, Research, Legal and Forensics, and DTC along with divisions for the implementation of technical and legal protections. Legal requirements and use cases in

state laws extend the potential areas of use into employment and insurance with legal protections needed throughout the process. In addition, the use lifecycle encompasses the retention and destruction aspects of storage beyond the presented framework.

Another pertinent issue is that consumers often do not have an understanding of the consequences of these DTC services [31]. In general, even when presented with consent agreements, consumers, patients and research participants have a wide variety of reasons for permitting access to their data, do not always fully understand the extent and implications of these agreements, and underestimate the ability for de-identification [7], [32], [33].

Rahmouni et al. developed an ontology of European privacy requirements for sharing patient data between countries [34], [35]. It focused on the implementation of data access between countries with respect to privacy status, consent requirements, recipients, level of detail, purpose, secondary purpose, and access by legal representatives. The consent requirements reflect many of the similar aspects in the US with respect to general areas such as when consent must be obtained, amount of details, written mode, and competency. These are divided up into four classes for necessity, specificity, explicitness, and format. There are no structures for the supplemental requirements prevalent in US laws outside various options for consent agreements and anonymization.

Other healthcare security focused ontologies lack the focus on purpose-driven access found in US laws. Blobel's pHealth has a policy structure that can implement many of the legal requirements and implements patient consent using policies [36]. The patient and internal organizational focus on access policies limits the opportunities to address the wide variety of scenarios prevalent with external access to patient data.

Most privacy models also use Role-Based Access Control (RBAC) to data inquiries and implementing enforcement policies. The use of RBAC has been identified as one of the candidates for implementing privacy access controls in the EHR domain [37], where rights can be assigned based on organizational policies in a hierarchical manner that is modified based on the user's role and then adjusted by the patient as desired. Healthcare privacy extensions, such as those proposed by Hung, provide the structure for adding concepts for areas including purpose, obligations, and retention [38]. The nature of genetic access restrictions and criteria requires a specific framework to accommodate the variations in state laws.

III. GENETIC PRIVACY ENFORCEMENT ONTOLOGY

A. Ontology Overview

The primary components of the genetic privacy ontology based upon Federal and State laws are the Requester, the Request and the Response as seen in Figure 1.

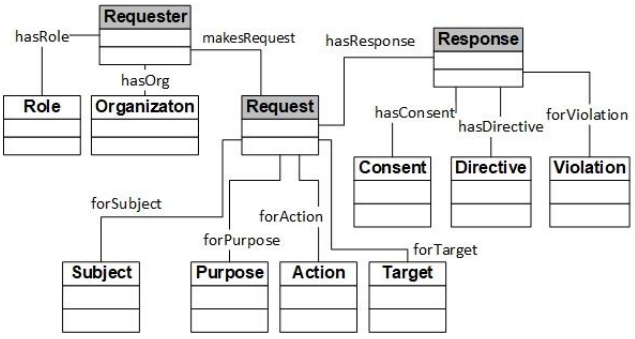

Figure 1. Genetic Privacy Ontology

- **Requester** addresses the person asking for access to the information and associated information such as their role and organization
- **Request** focuses on the purpose the Requester needs the information, the subject of the request (e.g., patient), what specific information is being sought (target), and what action will be performed with the information (e.g., read, retain, update).
- **Response** returns the answer to whether access is permitted or denied along with supplemental requirements for the release including if a consent form is required. The response includes reference material on the potential outcomes regarding a violation where the genetic information is incorrectly handled.

The first two (Requester and Request) are attribute based classes that can be used to generate an access decision (Permit or Deny) based on the Purpose-focused rules. For example, access to genetic information for medical purposes has a different set of permissions and requirements than those for law enforcement. These classes and associated rule base were previously addressed in detail and further information can be found in [18].

Once the access decision is made, then there are potentially a set of other requirements that are not attribute based but still need to be addressed. A Consent Form signed by the subject or their designated representative is often required and is usually generated for each specific request. There are also directives regarding a number of factors included in the state laws to address a large number of areas such as retention, use, supplemental disclosures, and de-identification. These directives may need to be addressed before release as a pre-condition, after release as a restriction on the use of the information, or obligations that the requester must perform after receipt. If the requester fails to adhere to these directives or the consent form directions, then the violation information provides insight into the penalties that can be assessed. The Consent, Directives and Violation classes are the focus of this paper.

B. Ontology Refinement

In our previous works, the ontology has been refined to reflect the increasing level of insights gathered. The first

ontology was developed based on related works review, other existing structures and ontologies, previous research in medical privacy, and the implementation of the laws for several initially selected sample states. The second published version of the ontology reflected adjustments to meet the requirements as more complex state laws were evaluated and compared against the work to date. As described in the methodology section, the efforts then moved to focus entirely on the ontology in order to fully address the state and federal laws specifically related to genetic medical privacy. The third published version reflected these efforts in the areas of Requester and Request classes.

This iteration addresses the criteria and actions to be taken to fulfill the request in accordance with the required conditions and constraints from the applicable Federal and State laws. The previous paper classified these actions into the following groupings:

- **Validations**: Pre-release activities (assuming all other permission criteria have been met) with two subclasses
- **Consen**t: Agreement from the subject or the appropriate representative to release the information along with specific clauses or text that must be included
- **Pre-conditions**: Requirements that must be addressed, completed or agreed to by the information provider or recipient such as ensuring the requester has a need to know
- **Constraints**: Post-release activities that the information recipient must agree to address
- **Restrictions**: Limits of the use, distribution or actions that can be taken with the information such as limiting re-disclosure based on the original purpose
- **Obligations**: Actions the recipient must take after receiving the information such as retention and destruction
- **Penalty**: Potential consequences for violating the validations or constraints associated with a specific rule.

This version of the ontology focusses on completing the analysis and classification of these components. The challenge and a major contribution have been the separation of pre-conditions and obligations. There are numerous instances where requirements are potentially applicable as both a pre-condition and obligation. For example, a "need to know" definitely implies that the current requester must fulfill the requirement as seen in the statement from Illinois Section 30, Disclosure of person tested and test results: Disclosure shall be limited to those who have a need to know the information, and no additional disclosures may be made. However, once the information is provided to the requester, it is a reasonable assumption (and may be required) that the requirement must also be applicable to re-disclosures. Therefore, Obligations and Pre-Conditions have been consolidated into a "Directives" class with attributes for Pre-Condition, Obligation and Restriction to provide additional flexibility during rule development. This change is reflected in the Figure 1.

Consent is a stand-alone class that reflect the specific characteristics of this requirement. While consent is typically thought of as a pre-release requirement, the analysis identified situations where this may occur post-release as well. For example, some states have a requirement that any re-disclosure or use for a different purpose requires additional consents. This condition must be enforced by the initial recipient. As seen in the sections below, notices that must be provided to the subject (or authorized signatory) with the consent are captured as a subclass to Consent. Since there are situations where notices are required based on the results of an information release, such as notices to parents about the results of neo-natal tests, these notices are captured within the Directives class structure.

Finally, some state laws directly state potential penalties associated with inappropriate genetic information release or use in the laws related to this subject. Therefore, a Violation class has been included to provide this information to the requester and reinforce the seriousness of complying with the relevant laws. There are a number of components, such as the violator's intent) to a violation in addition to the assessment of a specific penalty (such as a fine). Therefore, the class label was widened from Penalty to Violation to reflect these other subclasses.

C. Consent Super-Class

The Consent super-class shown in Figure 2 is more complex than simply providing a form for signature. In the analysis process, over 175 statements were extracted from laws regarding consents. State laws dictate a variety of specifications for signatories, format, text, informational notices, supplemental releases, record keeping and when consent is not required. The classes directly associated with the Consent super-class are:

- **Consent Form** represents the actual consent agreement and the associated requirements, directives, classes and notices to be provided. This Consent Form class is decomposed further below to provide information on various aspects.
- **Releases** addresses situations where additional consent may be required prior to the release of information regarding a specific individual or an institution. In the case where the request Purpose was Treatments, attributes flag when a physician must be the consent requester and the need

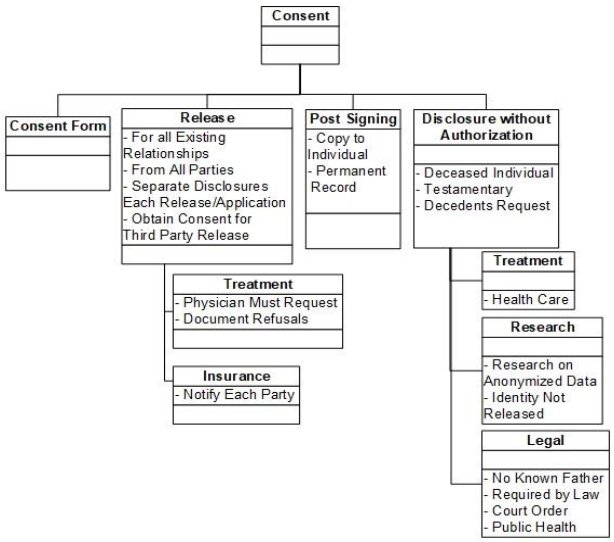

Figure 2. Consent Super-Class.

to document the refusal of a party to sign a consent statement. A requirement for insurance disclosures is to notify all the parties (or their guardian) in a group insurance of the conditions related to requesting genetic information.

- **Post-Signing** directs that the signed consent form must be included in the permanent record and/or a copy provided to the individual.
- **Disclosure Without Authorizations** outlines specific situations where genetic information may be eligible for release without the consent of the individual (or their representative). The three general conditions relate to a deceased individual while the other provide for release for medical treatment, specific types of research and legal conditions.

The Consent Form class in Figure 3 includes a number of attributes that reflect the conditions and requirements for the form itself. Because the focus here is genetic consent agreements, the Consent Form class also has an attribute to reflect the directions from some states that a general information release is not sufficient as seen in Georgia Statue 18.13.010: A general authorization for the release of medical records or medical information may not be construed as the informed and written consent required by this section. In these cases, another consent form that has specific criteria for genetic information must be signed even if there is a general release form on file. The classes associated with Consent Form are as follows:

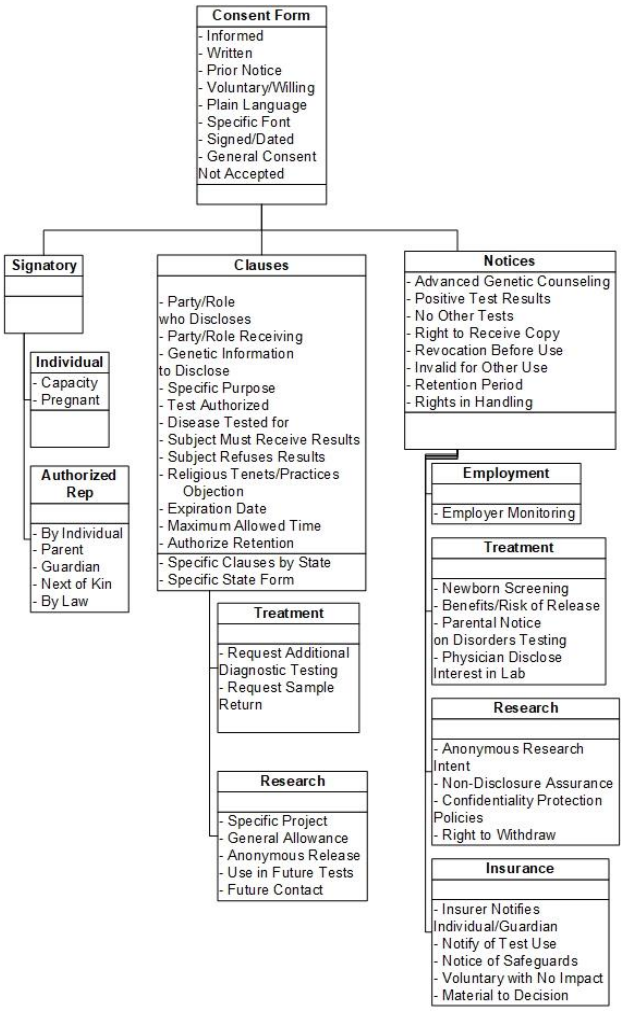

Figure 3. Consent Form Class.

- **Signatory** addresses who can sign the consent form. The individual can sign if they have the capacity (mental or age based). In Texas, a pregnant subject has additional consent requirements for any tests performed on a child in utero (as an implementation detail, these attributes would be reflected in the overall Subject class.) Authorized Representative may sign for individual and this representative may have been designated by the individual to sign on their behalf, may be the parent or guardian, a next of kin if the subject is deceased or set by some other criteria in the law.
- **Requirements** reflects specific statements in the laws regarding the consent form and overall process.
- **Clauses** provides the sections of text that must be included in the consent agreement being signed. Some states require that specific text or forms are used so this option is reflected as additional subclasses.
- **Notices** lists information that must be provided with the consent form. These disclosures provide additional information related to areas such as information use, rights of the subject, potential future use or disposition and participation in specific programs.

D. Directices Super-Class

Once the purpose-based rules are applied for a Requester to gain access based on the Request attributes, the Directives seen in Figure 4 dictate the pre-condition requirements for the release of information (in addition to consents), restrictions that are applied once the information is released, and obligations with specific actions that must be taken after the release. For example, a physician may be allowed to gain access to genetic information based on their role and their participation in a subject's treatment regimen. However, additional requirements might need to be addressed such as whether the physician has a need to know genetic information to provide care in the current use case. An Emergency Room doctor trying to access genetic information while treating a laceration might have to assert their Need to Know prior to gaining access. (Inappropriately asserting the need then becomes an external audit function and subject to the potentially involves the Penalty class.) These directives may not be retro-active so the date genetic information was obtained may be applicable in some states and use cases. These restrictions have been grouped into the following classes:

- **Disclosure** generally constrains the use of genetic information once permission rules are validated. (Releasing sub-sets of genetic information is addressed in the Limited class.) While some states may prevent additional disclosure under this request, other states provide specific criteria where re-disclosure is permitted which are addressed in a subclass.
- **Limited** provides criteria where disclosure of specific genetic information may be appropriate. AS opposed to Disclosure class, the Limited class addresses the ability for

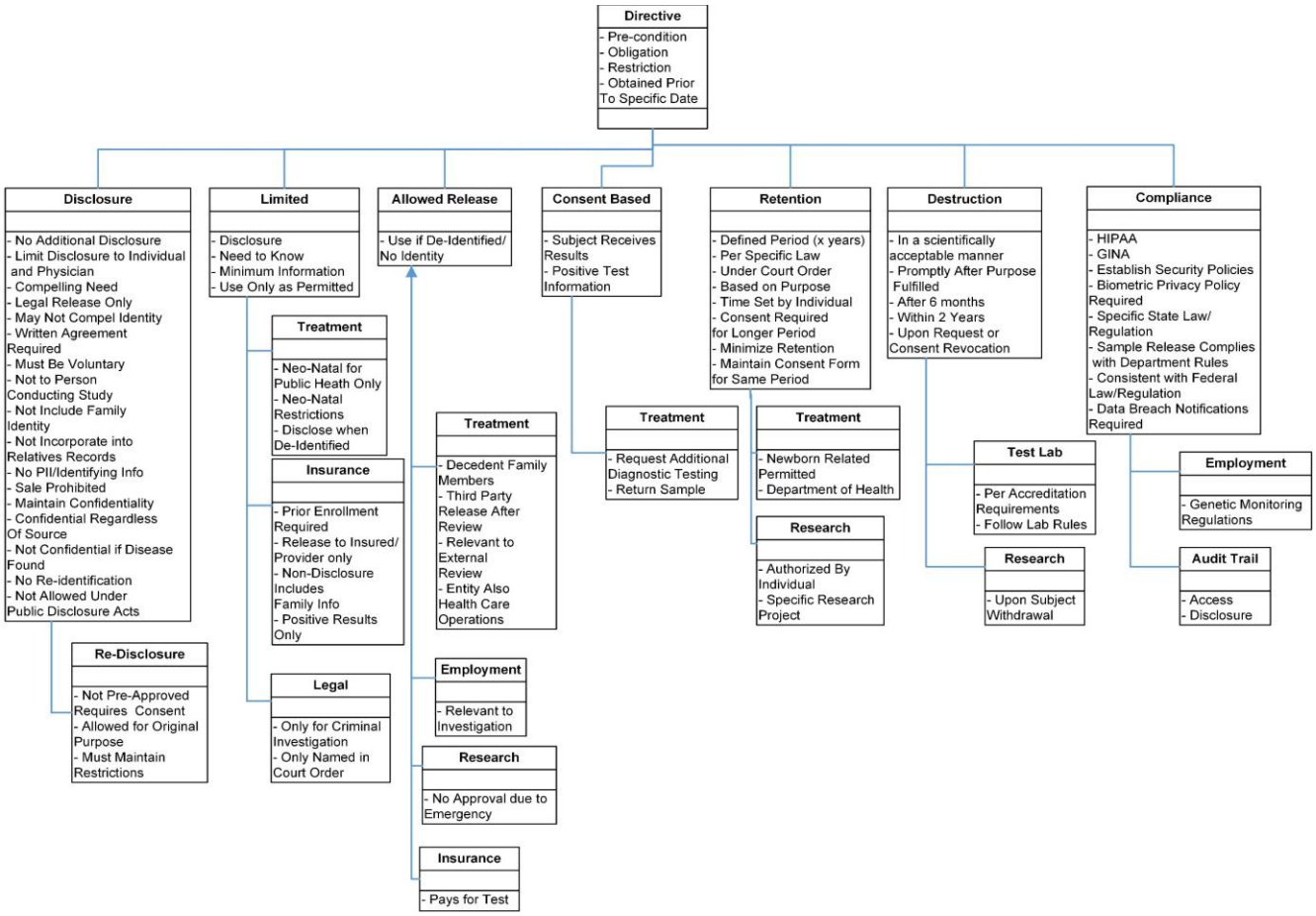

Figure 4. Directive Super-Class.

Disclosure to be for only a portion on the overall genetic information. Specific subclasses deal with situations that are only relevant to Treatment, Insurance or Legal based on the wording in the associated laws.

- **Allowed Release** addresses use cases where the law specifically states that information can be released. If Consent is required for an Allowed Release use case, the combination of Consent and Allowed Releases instances would be articulated in the relationships with the Release super-class.
- **Consent Based** reflects obligations and directives that must be enforced based on clauses and directives in the consent form.
- **Retention** specifies how long the genetic information may be retained either as specific time periods or general guidance. As an example of relationships between classes, Retention can be set by an individual with Authorize Retention as an option under Consent class.
- **Destruction** provides further direction on what to do when the retention period expires or upon a specific trigger. Test Labs have additional directions to follow practices determined by their accreditation requirements or lab guidelines. If a subject withdraws from a research project, destruction may be required depending on the state
- **Compliance** articulates state guidance to comply with certain laws, regulations or rules along with requiring policies and rules to be set related to the release of genetic information. In order to demonstrate compliance, some states provide specific guidance on recording access and disclosing audit records.

E. Violation Super-Class

As stated above, the Violation super-class shown in Figure 5 involves several aspects of addressing inappropriate release of genetic information as specific by Federal and State Laws. The following classes are under this category:

- **Intent** provides information on why the violator released the information. While the release may be Inadvertent, the penalties may be reduced as compared to a willful release.
- **Basis** describes the reasons or methods for the violation. These range from some type of gain (personal, corporate or otherwise) to wanting to inflect harm on someone.
- **Offense** separates out the criminal from non-criminal violations.
- **Actions** indicates how the violation will be addressed primarily for non-criminal offenses. (Criminal

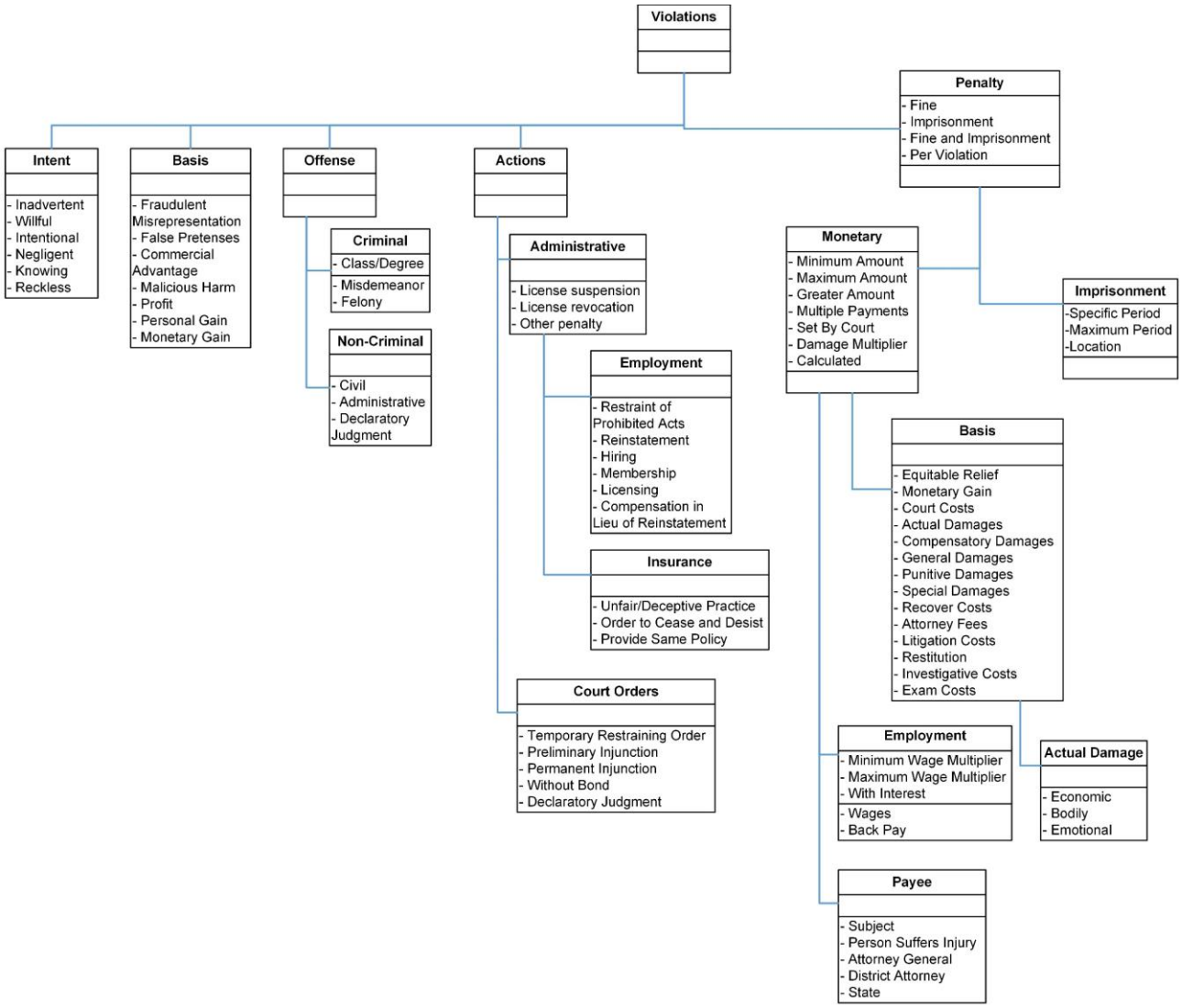

Figure 5.Violation Super-Class.

offenses may also trigger these actions but are not the primary focus in state laws.)

- **Penalty** indicates what the potential outcomes can be if a criminal offense is confirmed. The Penalty may be Monetary, Imprisonment, or a combination and there may be a penalty assessed for each violation.
  - **Monetary** has a number of attributes that may be associated with the assessed amount. In some cases, the amount may be set depending on a specific Basis. There are some penalties associated with Employment and the use of wages as a computational component. The Payee may be the Subject or some other party if not reimbursed back to the Government.
  - **Imprisonment** is usually set as a specific period to be served (in months or years) or a maximum amount. The location may be designated as a County or State facility.

F. Logical Definition Formulation

We provide a logical formulation to articulate the complexities of the genetic privacy protections in consideration of the wide variety of attributes and formulations that need to be specified in a hierarchical manner [39].

The core of the framework is a 5-tuple Data System (OTH, UGH, RH, A, Rel) where the elements are:

- OTH is an object-type hierarchy which in this case is an Electronic Health Record
- UGH is a user group hierarchy representing the system membership in the EHR
- RH is a role hierarchy for the role-based access permissions prevalent in the genetic information access requirements. For example, the HealthCare Provider role has subordinate roles such as the Physician and Nurse roles.

- A is the authorization nodes or Actions that can be performed on objects and is represented in the ontology as the Action super-class
- Rel is the set of relationships that links together element using unary, binary or n-ary tuples. For example, a medical record created by a physician is represented using a DidCreate(record, user) and thus will be provided additional access rights under the authorization component.

Within FAF, an authorization rule is in the form

$$\text{head}(o, s, \langle sign \rangle a) \leftarrow L_1 \& \cdots \& L_n.$$

where o is an object, s is a subject performing the actions, a is an action with the sign (+ or -) indicating permission or denial, and $L_1, \ldots, L_n$ are done, hie-, or rel-literals. done is a predicate stored in the history table, hie-literals are hierarchy predicates and rel-literals are application specific predicates. The rel-predicates provide the vehicle to address the majority of specifications found in the rule base.

However, within the context of accessing genetic information in an EHR, the cando tuple needs to be expanded to address the complexities found in a real-world situation. Therefore, cando is updated into shareable() to include the individual (i) patient's capacity to consent, the request (r) being made to obtain the purpose and state for the physical location, and the consent form (c) to determine if the individual has provided access. The revised formulation is

$$\text{shareable}(o,s,i,r, \langle sign \rangle a) \leftarrow L_1 \& \cdots \& L_n.$$

The set of rel-predicates includes:

- AllowedRole(r, s)
- AllowedOrg (r, s)
- PurposeAccess (o, a, r)
- needConsent(r,i)
- haveConsent (r,i)
- hasDirective (r, s)
- hasObligation (r, s)
- Precondition (r, s)
- WrittenForm (r)

If NeedConsent evaluates to true, then the haveConsent predicate is evaluated based on the following:

haveConsent() ← giveConsent(r,i), ConsentOnFile(r,i)
noConsent() ← ¬giveConsent(r,i), ¬ConsentOnFile(r,i)

The final decision is evaluated as follows to address any conflicts:

finalConsentDecision() ← haveConsent(), ¬ noConsent()

In addition, the negation of a predicate indicates that some aspect is not needed within this context. For example, if consent is not required (as is common for law enforcement requests), then ¬NeedConsent(r,i) indicates that the individual's consent is not required for this request.

In a similar manner to cando in FAF, dercando is updated to dershareable to implement two areas where authorization is derived from inferences. giveConsent can potentially be a hierarchical situation where multiple consents may be present that must be evaluated.

For example, in some cases a minor child can give permission without their parent's approval. Alternatively, there are other scenarios where the parents can provide consent that overrides the minor's directives. In addition, permissions granted to one part of a medical record will be inherited by related or "lower" aspects of the record. The person who requested a genetic test is often provided access to the test results by inheritance. If consent is provided to all genetic information within the record to the physician, it is obvious this permission is inherited by all genetic-related information.

IV. IMPLEMENTATION

Our previous work included a prototype that uses a workflow engine to gather the required attributes, display the results and confirm the implementation of the directives [17], [18]. These papers include additional information on the specific steps in the workflow and the overall development process along with screen shots and the rules algorithm.

The workflow engine, Yet Another Workflow Language (YAWL), is compatible with Electronic Health Record (EMR) systems such as OpenMRS [40]. This integration will allow many of the attributes about the request and requester to be directly extracted from the record repository. In addition, the prototype will force a consent to be obtained in case of need. As seen in Figure 6, these attributes are then extracted by the Consent Service and the Protégé ontology populated for the execution of the rules. The results are processed by the Rules Hierarchy Algorithm, and Consent Service to develop the Final Access Results. The results also include any associated pre-conditions, obligations, restrictions and violations that are part of the enforcement component. These results are returned to the workflow for display of the access decision along with a confirmation that the consent has been completed along with agreement the directives have been evaluated and addressed.

The workflow process is shown in Figure 7. Section 1 of the workflow gathers the required attributes and generates the

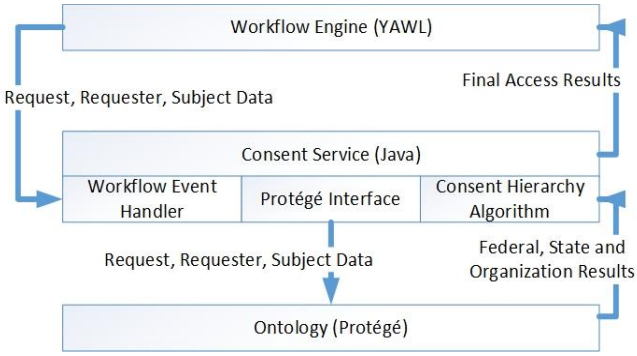

Figure 6. Prototype Architecture.

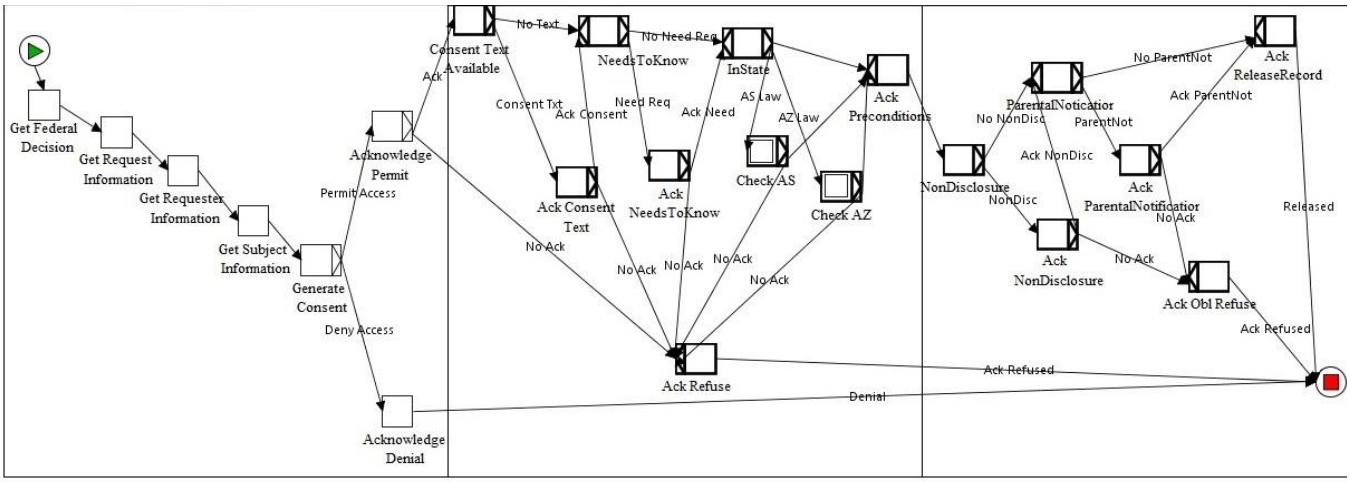

Figure 7. Prototype Workflow.

access decision. Section 2 displays the complete set of results and requests a confirmation. The next set of steps generates the consent agreement and requests an electronic signature. Once the consent agreement is signed, the directives identified as pre-conditions are displayed and the requester validates that the conditions have been met. Once the pre-conditions are met, the restrictions and obligations are provided to be enforced as part of the release process. Failing to complete any of the steps or provide the necessary signatures/agreements in Sections 2 and 3 will result in the access decision converting to a Deny.

A. SWRL Rule Structure

This section specifies the rule structure for all access inquiry rules and the associated release conditions in the Protégé prototype [16], [17]. The workflow captures the required data elements and the Consent Service populates the Protégé ontology instances with the submitted data. The workflow has three steps to collect the access inquiry information on the request, requester and subject as described in our previous papers. The SWRL rule structure defines how the ontology-based rules are built in order to provide an access decision along with any applicable response details for consent, directives and violations. (The structure is provided in Figure 1.)

Basic Structure

At a minimum, each rule must have a request, requester and response. In addition, any required response condition instances (consent, directives and violations) are retrieved in the precedent for use in the antecedent.

- **g(inquiry), f(request), f(requester), g(response), g(conditions) -> s(response), s(conditions)**

The g() predicates get the instances from the ontology for evaluation or use in the response. The f() predicates then evaluate the instances to determine if the rule is applicable for this access request. The s() functions in the antecedent sets the response instance attributes and associates the retrieved conditions with the response.

g(inquiry) retrieves the required instances present in all rules for both the request and requester instances with one statement.

- **makesRequest(?r, ?req**) which provides the linked request and requester instances.

f(request) and f(requester) provide the predicates for evaluating if the rule is applicable to the access inquiry. Since these two functions encompass the entire rule base, selected functions are provided to illustrate their operation.

One example is to restrict the rule enforcement to a specific state. The following predicate operates on an attribute in the request instance.

- **inState(?req, abbr)** where abbr is the two letter state abbreviation such as “DE” for Delaware.

If the rule is enforcing a constraint in a subclass to the requester (role or organization) or request (subject, purpose, action or target), the function first retrieves the associated instance and then performs the evaluation.

- **forResource(?req,?resource), isGeneticResult(?resource, true)** which is used to determine the specific part of the medical record that is being accessed (forResource) and if the record component contains genetic information based on a resource attribute (isGeneticResult).
- **forPurpose(?req, ?pur), isTreatment (?pur, true)** where an Purpose instance (forPurpose) attribute (isTreatment) is evaluated to determine if the purpose is in a specific grouping. In this example, all medically oriented treatment purposes are grouped in the isTreatment property on the Purpose.

g(response) is comprised of two SWRL statements because there are three separate response objects that can be associated with each access inquiry for the Federal, State and Organization levels. The objects are respectively ?res, ?resst and ?resorg to match the three levels. Each rule only contains one response instance and the correct response level is obtained using one of these combinations:

- **hasResponse(?req, ?res), responseLevel(?res, "Federal")**

- **hasResponse(?req, ?resst), responseLevel(?resst, "State")**
- **hasResponse(?req, ?resorg), responseLevel(?resorg, "Org")**

g(condition) gets the instances that will be used in the antecedent to establish the conditions associated with the information release. The instances are obtained from the Consent, Directive and Violation super-classes and all subclasses that reflect the release requirements. For example, one requirement often imposed by states is that the requester must have a "need to know" in order to be permitted access to the genetic information. In the first step, the "Need to know" instance is retrieved in the following rule snippet. Under s(condition) the instance is associated with the state response.

- **oblName(?pre, "NeedToKnow")** is used to retrieve the Directive instance with the name "NeedToKnow" and then associate this instance with ?pre. ?pre is used in s(response) to enforce the requirement.

Multiple conditions are associated with one rule by creating unique instances to replace ?pre in the formula. For example, ten consent clauses can be associated with one rule by replacing ?pre with ?clause1…?clause10.

s(response) sets the response instance attributes to reflect if access is permitted and provide supporting information on the basis of the access decision. The assignment statements are:

- **isAllowed(?resst, boolean)** to set the access decision to permit (true) or deny (false)
- **canOverride(?resst, boolean)** to communicate if "lower" level rules can override this rule. For example, if the State law permits access, an override of false means the organization can't deny access.
- **decisionSource(?resst, text)** to provide the reference information for the rule from the applicable law, regulation or policy.
- **hasRule(?resst, integer)** is an implementation specific construct to simplify debugging and gives each rule a unique ID

s(condition) uses relationship statements to associate the previously retrieved conditions with the response instance.

- **hasPreCondition(?resst, ?pre)** takes the ?pre instance retrieved for the NeedToKnow example and uses hasPreCondition to associate the condition with the ?resst release instance obtained under g(release).

Simple Rule Example

In this SWRL rule, a person is allowed access to their own medical records for information regarding genetic test results. This rule implements a portion of a Georgia State Law: Information derived from genetic testing shall be confidential and privileged and may be released only to the individual tested.

makesRequest(?r, ?req), isSelf(?r, true), inState(?req, ""GA""), forResource(?req, ?resource), isGeneticResult(?resource, true), forPurpose(?req, ?pur), purposeDesc(?pur, ""SelfRequest""), hasResponse(?req, ?resst), responseLevel(?resst, ""State"") -> isAllowed(?resst, true), canOverride(?resst, false), decisionSource(?resst, ""GA LAW 33-54-3""), hasRule(?resst, 10)"

g(inquiry): makesRequest(?r, ?req)
f(request): inState(?req, ""GA""),
forResource(?req, ?resource),
isGeneticResult(?resource, true),
forPurpose(?req, ?pur), purposeDesc(?pur, ""SelfRequest""),
f(requester): isSelf(?r, true),
g(response): hasResponse(?req, ?resst),
responseLevel(?resst, ""State""),
s(response): isAllowed(?resst, true),
canOverride(?resst, false),
decisionSource(?resst, ""GA LAW 33-54-3""),
hasRule(?resst, 10)"

Note there are no conditions associated with this rule since the law does not impose any restrictions.

V. RESPONSE EXAMPLE

The following snippets from Delaware State Law Chapter 12, Informed Consent and Confidentiality, provides an example that would be applicable to a request for medical treatment:

> *(a)No person shall obtain genetic information about an individual without first obtaining informed consent from the individual.*
>
> *(4) Informed consent"*
>
> *a. For the purpose of obtaining genetic information, means the signing of a consent form which includes a description of the genetic test or tests to be performed, its purpose or purposes, potential uses, and limitations and the meaning of its results, and that the individual will receive the results unless the individual directs otherwise;*
>
> *(a) Regardless of the manner of receipt or the source of genetic information, including information received from an individual, a person shall not disclose or be compelled, by subpoena or any other means, to disclose the identity of an individual upon whom a genetic test has been performed or to disclose genetic information about the individual in a manner that permits identification of the individual, unless…:*
>
> *(b) Any person who willfully obtains or discloses genetic information in violation of this subchapter shall be punished by a fine not less than $5,000 not more than $50,000.*

A. SWRL Rule

A sample SWRL rule that would be invoked for this scenario is as follows:

makesRequest(?r, ?req), inState(?req, "DE"), forResource(?req, ?resource), isGenetic(?resource, true), forPurpose(?req, ?pur), isTherapeutic(?pur, true), hasResponse(?req, ?resst), responseLevel(?resst, "State"), oblName(?consent, "ConsentRequired"), oblName(?dir, "MayNotCompelIdentity"), vioName(?vio, "Willfull") -> isAllowed(?resst, true), canOverride(?resst, false), hasConsent(?resst, ?consent), isSigned(?consent, true), isDescription (?consent, true), isPurpose(?consent, true), ?isUse(?consent, true),

?isPositiveTestResults(?consent, true), isSubjectReceivesResults(?consent, true), hasDirective (?resst, ?dir), forViolation(?resst, ?vio), isMin(?vio, 5000), isMax(?vio, 50000), decisionSource(?resst, "DE LAW 12"), hasRule(?resst, 1200)

In this rule,

- **?r** is for the Requester of the Request
- **?req** is for the Request that links the various components, such as Subject, Purpose and Resource
- **?pur** is the Therapeutic Purpose that is associated with the Request
- **?resource** is for the "GeneticTestResults" part of the medical record
- **?consent** is for the Consent Required clause
- **?dir** is the Directive that the recipient may not be compelled to reveal the subject's identity.
- **?vio** is the Willful Violation object
- **?resst** is the State Response object that is associated with the Request.

These SWRL statements are explained in Table I.

TABLE I. SAMPLE RESPONSE STATEMENT RULE

SWRL Statement	***Explanation***
makesRequest(?r, ?req)	Links Requester for the Request
inState(?req, "DE")	Request is for Delaware
forResource(?req, ?resource)	Links Request with the Resource
isGenetic(?resource, true	Restricts the rule to a Resource that is identified as a genetic information
forPurpose(?req, ?pur)	Links Request with Purpose
isTherapeutic(?pur, true)	Restricts the rule to a Treatment Purpose
hasResponse(?req, ?resst)	Links the Request with a Response to store answer
responseLevel(?resst, "State")	Gets the Response for State level to store answers
oblName(?consent, "ConsentRequired")	Gets the Consent Required Object
oblName(?dir, "MayNotCompelIdentity")	Gets the appropriate Directive object
vioName(?vio, "Willfull")	Gets the appropriate Violation object
-> isAllowed(?resst, true)	Sets the State response to access is allowed
canOverride(?resst, false)	Sets the state Response to not allow override by organization
hasConsent(?resst, ?consent)	Sets the State response to include the Consent Required condition
isSigned(?consent, true), isDescription (?consent, true), isPurpose(?consent, true), ?isUse(?consent, true), ?isPositiveTestResults(?consent, true), isSubjectReceivesResults(?consent, true)	Sets the attributes on the Consent object to require a signed form that includes the description, purpose, use, test results meaning and subject receiving results
hasDirective (?resst, ?dir)	Sets the State response to include the MayNotCompelIdentity obligation
forViolation(?resst, ?vio)	Sets the State response to include the Wilful Violation
isMin(?vio, 5000), isMax(?vio, 50000)	Sets the Minimum and Maximum Fine amounts for the Violation
decisionSource(?resst, "DE LAW 12")	Sets the State response to reflect the decision source as state law
hasRule(?resst, 1200)	Sets the rule number to 1200 for reference

B. Obligation Enforcement

Once the genetic information has been released, obligations then require additional interactions in order to enforce the applicable laws, regulations and consent directives. A YAWL workflow is presented in Figure 8 to address the required process. A trigger in the underlying EHR invokes the workflow and creates a workflow item for evaluation. A workflow path then is selected from the following list to execute the associated rules:

- **Re-disclosure Request** determines if further dissemination is permitted based on the original request. There are three identified conditions where additional consent may be required, the re-disclosure can be performed if the purpose is the same as the original request, and only if the original restrictions are agreed upon for the release.
- **Test Results Received** from a genetic test request is evaluated for specific conditions associated with the original request and consent form. Subject notification may be required that the results were received. As a separate workflow, the subject may be entitled to additional information if the test is positive for the condition.
- **Retention Expired** begins the review process to determine if the genetic information/sample can be retained longer. If the criteria are met, then the retention period can be extended. Otherwise the information and/or sample is subject to destruction. For samples, the destruction may be subject to

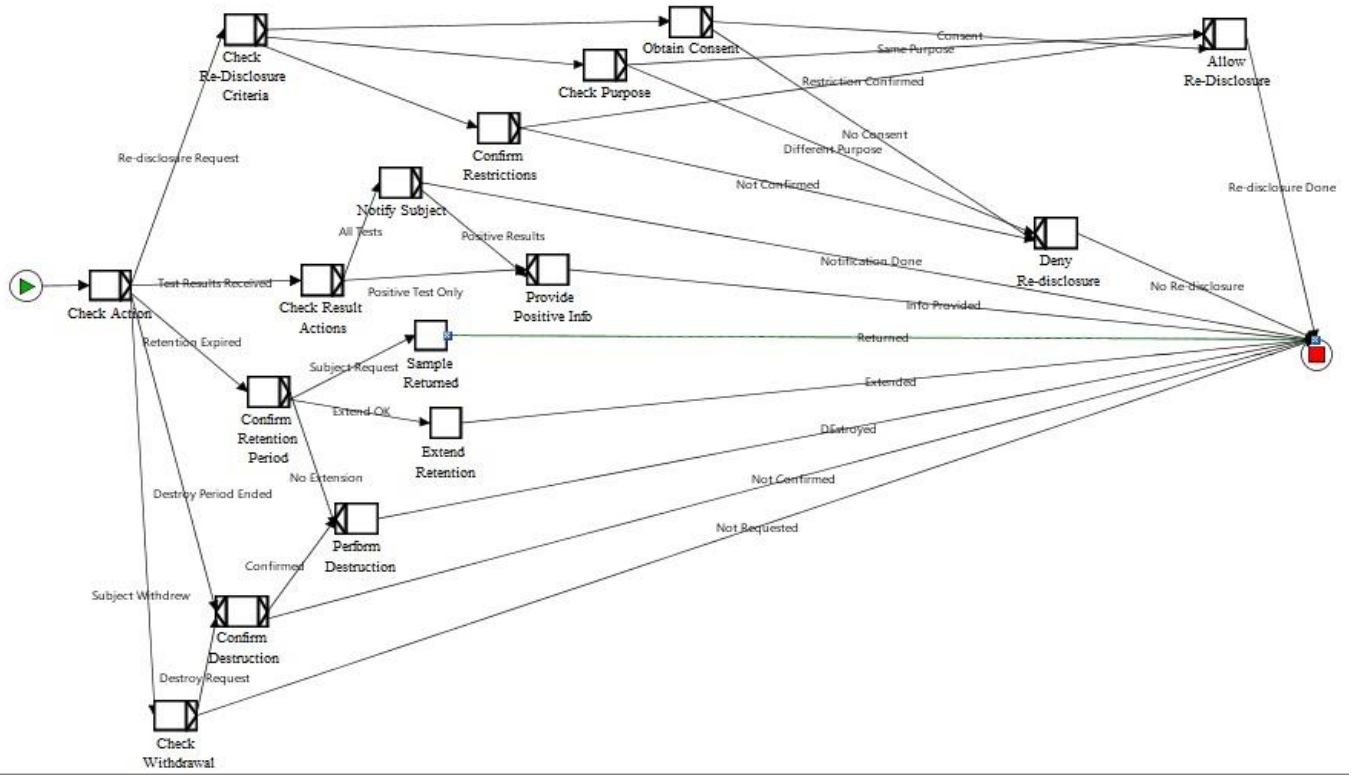

Figure 8. Obligation Workflow.

specific requirements or, if stated in the consent agreement stated, the sample must be returned to the subject.

- **Destroy Period Ended** indicates the time has expired and the sample must be destroyed in accordance with any specified processes.
- **Subject Withdrew** from a research project may impact the sample and trigger a destruction action.

C. Obligation Example

The following snippets from Nevada State Law Chapter 629.161, Retention of genetic information that identifies person without consent unlawful; exceptions; destruction of genetic information, provides an example that would be applicable to destruction for a subject withdrawing from a research study:

> *3. Except as otherwise provided in subsection 4 or by federal law or regulation, a person who obtains the genetic information of a person for use in a study shall destroy that information upon:*
>
> *(a) The completion of the study; or*
>
> *(b) The withdrawal of the person from the study, whichever occurs first.*
>
> *4. A person whose genetic information is used in a study may authorize the person who conducts the study to retain that genetic information after the study is completed or upon his or her withdrawal from the study.*

The following snippets from Nevada State Law Chapter 629.191, Penalty, indicates the outcome for a failure to comply with the previous clause:

> *A person who violates any of the provisions of NRS 629.151, 629.161 or 629.171 is guilty of a misdemeanor.*

A sample SWRL rule that would be invoked for a subject that has not agreed to have the information retained upon withdrawal from a research study is as follows:

madeRequest(?r, ?req), inState(?req, "NV"), forResource(?req, ?resource), isGenetic(?resource, true), forPurpose(?req, ?pur), isResearch(?pur, true), isResearch(?resource, true), forSubject(?sub, ?req), hasAction(?sub, "WithDrew"), hasConsent(?sub, ?consent), hasRetainWithdraw (?consent, ?clause), isRetainAllowed(?clause, false), responseLevel(?resst, "State"), oblName(?obl, "DestroyInfo"), degreeName(?degree, "Misdemeanor") -> hasObligation (?resst, ?obl), forViolation(?resst, ?degree) , decisionSource(?resst, "NV LAW 629.161"), hasRule(?resst, 1201)

In this rule, the following instances are added from the previous example:

- ?sub is for the Subject of the Request
- ?consent represents the Consent Agreement with the Subject
- ?clause are the clauses in the Consent Agreement

• ?obl is the obligation that the organization must fulfill

• ?degree provides the class/degree associated with this criminal offense if the information is not destroyed

These SWRL statements are explained in Table II.

TABLE II. SAMPLE OBLIGATION RULE

SWRL Statement	***Explanation***
madeRequest(?r, ?req)	Links Requester for the original Request
inState(?req, "NV")	Request is for Nevada
forResource(?req, ?resource)	Links Request with the Resource
isGenetic(?resource, true	Restricts the rule to a Resource that is identified as a genetic information
forPurpose(?req, ?pur)	Links Request with Purpose
isResearch(?pur, true)	Restricts the rule to the Research Purpose
forSubject(?sub, ?req)	Obtains the Subject associated with the Request
hasAction(?sub, "WithDrew")	Indicates the Subject has the Action for Withdrew
hasConsent(?sub, ?consent)	Obtains the Consent Agreement for this Subject
hasRetainWithdraw (?consent, ?clause)	Restricts the Rule to the Subject having the Clause to Retain Information upon Withdrawal
isRetainAllowed(?clause, false)	Determines that the Retention is set to false
hasResponse(?req, ?resst)	Links the Request with a Response to store answer
responseLevel(?resst, "State")	Gets the Response for State level to store answers
oblName(?obl, "DestroyInfo")	Gets the Obligation to Destroy Info
degreeName(?degree, "Misdemeanor")	Gets the appropriate degree object
->hasObligation(?resst, ?consent)	Sets the State response to Destroy Info
forViolation(?resst, ?degree)	Sets the State response as the Misdemeanour Violation
decisionSource(?resst, "NV LAW 629.161")	Sets the State response to reflect the decision source as state law
hasRule(?resst,1201)	Sets the rule number to 1201 for reference

Upon receiving this result, the workflow would advance to the destruction path to implement the clauses in the subject's consent agreement.

VI. CONCLUSION AND FUTURE WORK

Our genetic privacy ontology was built directly from the applicable Federal and State laws without any pre-conceived boundaries or required elements. The work demonstrates the importance of a purpose-focused structure to appropriately link the various data elements necessary to permit or deny access to the genetic medical information. The ontology and previous prototype work allows the data collection to be directly integrated into EHRs. The next step will be validating an integrated EHR, ontology and prototype using operational data and genetic data requests to demonstrate the appropriate data protections are enforced. This comprehensive integration reduces the provider's effort and provides access decisions in accordance with relevant laws, policies and regulations.

REFERENCES

[1] M. Reep, B. Yu, D. Wijesekera, and P. Costa, "An Ontology for Specifying Regulation-Compliant Genetic Privacy Policies," in *eTELEMED 2018, The Tenth International Conference on eHealth, Telemedicine, and Social Medicine*, 2018, pp. 66–74.

[2] K. Wuyts, R. Scandariato, G. Verhenneman, and W. Joosen, "Integrating Patient Consent in e-Health Access Control," *Int. J. Secure Softw. Eng.*, vol. 2, no. 2, pp. 1–24, 32 2011.

[3] J. Pritts, "The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research." Institute of Medicine, 2008.

[4] M. H. Ullman-Cullere and J. P. Mathew, "Emerging landscape of genomics in the electronic health record for personalized medicine," *Hum. Mutat.*, vol. 32, no. 5, pp. 512–516, May 2011.

[5] M. D. Ritchie, E. R. Holzinger, R. Li, S. A. Pendergrass, and D. Kim, "Methods of integrating data to uncover genotype-phenotype interactions," *Nat. Rev. Genet.*, vol. 16, no. 2, pp. 85–97, Feb. 2015.

[6] C. Pihoker *et al.*, "Prevalence, Characteristics and Clinical Diagnosis of Maturity Onset Diabetes of the Young Due to Mutations in HNF1A, HNF4A, and Glucokinase: Results from the SEARCH for Diabetes in Youth," *J. Clin. Endocrinol. Metab.*, vol. 98, no. 10, pp. 4055–4062, Oct. 2013.

[7] Y. M. Lee, R. P. McKillip, B. A. Borden, C. E. Klammer, M. J. Ratain, and P. H. O'Donnell, "Assessment of patient perceptions of genomic testing to inform pharmacogenomic implementation," *Pharmacogenet. Genomics*, vol. 27, no. 5, pp. 179–189, May 2017.

[8] B. M. Knoppers, "Genetic information and the family: are we our brother's keeper?," *Trends Biotechnol.*, vol. 20, no. 2, pp. 85–86, Feb. 2002.

[9] S. Dheensa, A. Fenwick, S. Shkedi-Rafid, G. Crawford, and A. Lucassen, "Health-care professionals' responsibility to patients' relatives in genetic medicine: a systematic review and synthesis of empirical research," *Genet. Med.*, vol. 18, no. 4, pp. 290–301, Apr. 2016.

[10] S. B. Trinidad, T. B. Coffin, S. M. Fullerton, J. Ralston, G. P. Jarvik, and E. B. Larson, "'Getting off the Bus Closer to Your Destination': Patients' Views about Pharmacogenetic Testing," *Perm. J.*, vol. 19, no. 3, pp. 21–27, 2015.

[11] W. W. Lowrance, "Privacy, Confidentiality, and Identifiability in Genomic Research." Discussion document for workshop convened by the National Human Genome Research Institute, Bethesda, Oct-2006.

[12] M. Gymrek, A. L. McGuire, D. Golan, E. Halperin, and Y. Erlich, "Identifying Personal Genomes by Surname Inference," *Science*, vol. 339, no. 6117, pp. 321–324, Jan. 2013.

[13] O. for C. Rights (OCR), "Privacy Rule General Overview," *HHS.gov*, 05-Nov-2015. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/general-overview/index.html. [Accessed: 01-Jun-2019].

[14] O. for C. Rights (OCR), "Genetic Information," *HHS.gov*, 07-May-2008. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html. [Accessed: 01-Jun-2019].

[15] A. A. Lemke *et al.*, "Patient perspectives following pharmacogenomics results disclosure in an integrated health system," *Pharmacogenomics*, Feb. 2018.

[16] "State and Federal Consent Laws Affecting Interstate Health Information Exchange." [Online]. Available: https://classic.nga.org/cms/home/nga-center-for-best-practices/center-divisions/center-issues/page-health-issues/data-and-analytics/col2-content/list--right/resources/content-reference@/state-and-federal-consent-laws-a.default.html. [Accessed: 01-Jun-2019].

[17] M. Reep, B. Yu, D. Wijesekera, and P. Costa, "Sharing Data under Genetic Privacy Laws," in *Proceedings of the Eleventh Conference on Semantic Technology for Intelligence, Defense, and Security*, Fairfax VA, USA, 2016, pp. 46–54.

[18] M. Reep, B. Yu, D. Wijesekera, and P. Costa, "Sharing Genetic Data under US Privacy Laws," in *11th International Joint Conference on Biomedical Engineering Systems and Technologies*, Funchal, Madeira, Portugal, 2018, vol. 5: HEALTHINF, pp. 349–360.

[19] "Enabling Document Sharing Using IHE Profiles - IHE Wiki." [Online]. Available: http://wiki.ihe.net/index.php/Enabling_Document_Sharing_Using_IHE_Profiles. [Accessed: 01-Jun-2019].

[20] "Basic Patient Privacy Consents - IHE Wiki." [Online]. Available: http://wiki.ihe.net/index.php?title=Basic_Patient_Privacy_Consents. [Accessed: 01-Jun-2019].

[21] J. Kaye, E. A. Whitley, D. Lund, M. Morrison, H. Teare, and K. Melham, "Dynamic consent: a patient interface for twenty-first century research networks," *Eur. J. Hum. Genet.*, vol. 23, no. 2, pp. 141–146, Feb. 2015.

[22] Y. Erlich *et al.*, "Redefining Genomic Privacy: Trust and Empowerment," *PLOS Biol.*, vol. 12, no. 11, p. e1001983, Nov. 2014.

[23] T. G. A. for G. and Health*, "A federated ecosystem for sharing genomic, clinical data," *Science*, vol. 352, no. 6291, pp. 1278–1280, Jun. 2016.

[24] "Global Alliance for Genomics and Health: Privacy and Security Policy." Global Alliance for Genomics and Health, 26-May-2015.

[25] "Standards and implementation practices for protecting the privacy and security of shared genomic and clinical data." Global Alliance for Genomics and Health, 09-Aug-2016.

[26] B. M. Knoppers, "Framework for responsible sharing of genomic and health-related data," *HUGO J.*, vol. 8, no. 1, p. 3, Dec. 2014.

[27] admin, "Protecting Data, Promoting Access: Improving Our Toolbox," *Office of Science Policy*, 02-May-2016.

[28] S. O. M. Dyke *et al.*, "Consent Codes: Upholding Standard Data Use Conditions," *PLoS Genet.*, vol. 12, no. 1, Jan. 2016.

[29] "HL7 Version 3 Standard: Security and Privacy Ontology, Release 1." Health Level Seven International, May-2014.

[30] M. Naveed *et al.*, "Privacy in the Genomic Era," *ACM Comput Surv*, vol. 48, no. 1, pp. 6:1–6:44, Aug. 2015.

[31] H. Shen and J. Ma, "Privacy Challenges of Genomic Big Data," in *Healthcare and Big Data Management*, Springer, Singapore, 2017, pp. 139–148.

[32] J. M. Oliver, M. J. Slashinski, T. Wang, P. A. Kelly, S. G. Hilsenbeck, and A. L. McGuire, "Balancing the Risks and Benefits of Genomic Data Sharing: Genome Research Participants' Perspectives," *Public Health Genomics*, vol. 15, no. 2, pp. 106–114, 2012.

[33] T. Haeusermann, B. Greshake, A. Blasimme, D. Irdam, M. Richards, and E. Vayena, "Open sharing of genomic data: Who does it and why?," *PLoS ONE*, vol. 12, no. 5, p. e0177158, May 2017.

[34] H. B. Rahmouni, T. Solomonides, M. C. Mont, S. Shiu, and M. Rahmouni, "A Model-driven Privacy Compliance Decision Support for Medical Data Sharing in Europe," *Methods Inf. Med.*, vol. 50, no. 4, pp. 326–336, 2011.

[35] H. B. Rahmouni, T. Solomonides, M. C. Mont, and S. Shiu, "Privacy compliance and enforcement on European healthgrids: an approach through ontology," *Philos. Trans. R. Soc. Lond. Math. Phys. Eng. Sci.*, vol. 368, no. 1926, pp. 4057–4072, Sep. 2010.

[36] B. Blobel, "Ontology driven health information systems architectures enable pHealth for empowered patients," *Int. J. Med. Inf.*, vol. 80, no. 2, pp. e17–e25, Feb. 2011.

[37] F. Falcao-Reis, A. Costa-Pereira, and M. Correia, "Access and privacy rights using web security standards to increase patient empowerment," in *Medical and Care Compunetics 5*, vol. 137, IOS Press, 2008, pp. 275–285.

[38] P. Hung and Y. Zheng, "Privacy Access Control Model for Aggregated e-Health Services," *EDOC Conf. Workshop 2007 EDOC 07 Elev. Int. IEEE*, no. 15-16 Oct. 2007, pp. 12–19, Jul. 2008.

[39] S. Jajodia and D. Wijesekera, "A Flexible Authorization Framework for E-Commerce," in *Distributed Computing and Internet Technology*, 2004, pp. 336–345.

[40] W. M. P. van der Aalst and A. H. M. ter Hofstede, "YAWL: yet another workflow language," *Inf. Syst.*, vol. 30, no. 4, pp. 245–275, Jun. 2005.