An Ontology for Specifying Regulation-Compliant Genetic Privacy Policies

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— **Genetic information provides important diagnostic data from patients to their health care providers and researchers that match phenotype and genotype. However, both diagnostic and research data providers must be confident that using this data for either purpose protects the data provider from foreseeable privacy breaches. In order to do so, Federal and State laws are in place to specifically address genetic information in addition to the laws established to protect generic health information. State genetic privacy laws diverge widely in their level of detail and constraints on releasing data, criteria for evaluating access to such data, data owner consents required to release data, and conditions for using released data. A rule-base specifying these variations can be used as a policy language to enforce data releases from electronic health records and gene pools. In order to satisfy this need, we describe a comprehensive ontology for genetic privacy based on existing applicable laws. Our ontology is used in ontological rule bases within medical workflows that are directly integrated with electronic health records. As shown in our ongoing work, this integration provides a solid foundation for enforcing laws and regulations in preventing unlawful disclosures of genetic information.**

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

I. INTRODUCTION

Patients are less likely to share data if there is a concern about privacy, so consents are necessary to help allay these concerns [1]. Privacy concerns have been heightened as Electronic Health Records (EHRs) have become widespread and ensuring privacy has increased in importance [2][3]. The privacy concerns that patients have about electronic medical records also apply to genetic information. 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 and treatment costs [4][5]. 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 [6]. 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 [7][8].

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 [9]. HIPAA was also followed by the Genetic Information Nondiscrimination Act of 2008 (GINA) to protect individuals from discrimination in employment and insurance based on genetic information [10]. Furthermore, almost every state and the District of Columbia have laws that specifically address genetic protections to some degree. Health Information Exchanges and direct sharing between health care providers are still subject to the applicable State laws even for interstate data transfers [11]. This paper 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 structured formal 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. Workflows provided the mechanism to gather the necessary information within the context of an EHR. We prepared an initial genetic privacy ontology and sample rules to enforce laws in selected states to validate our approach.

Our next step is developing this comprehensive genetic privacy ontology based directly on relevant Federal and State laws. Following this Introduction, Section 2 addresses related work; Section 3 provides the methodology we followed in developing this ontology; Section 4 describes the genetic privacy ontology with detailed descriptions for each super-class; Section 5 provides an example of the ontology being used in our prototype; and, finally, Section 6 presents conclusions.

II. RELATED WORKS

There are existing standards and frameworks with methods to implement various aspects of genetic privacy protections. The Integrating the Healthcare Enterprise (IHE)

 ISBN: 978-1-61208-618-7

standards profiling organization has developed frameworks, use cases, and specifications for managing the sharing of documents between organizations [12]. The inter-organizational policies must be completed prior to the use of this standard for implementing the consent agreements. There is some capability to address components of genetic privacy related to acknowledging consents but not all the required capability. 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 [13]. Many State laws call for this type of consent specifications as a prerequisite for permissible access to data.

The restrictions placed by regulatory environments on information sharing has been identified as an issue that requires coordination across system silos [14]. 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 [15][16]. 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 [17]. 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.

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 State law implementation requirements. The HL7 Security and Privacy Ontology has a class *PurposeOfUseOntology* with a purpose code and description [18, p. 1]. 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. 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. 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. But consumers often do not have an understanding of the consequences of these services [19]. 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 [20][21] .

Work by Rahmouni *et al.* developed an ontology of European privacy requirements for sharing patient data between countries [22][23]. 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. 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 [24]. 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 [25], 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 [26]. The nature of genetic access restrictions and criteria requires a specific framework to accommodate the variations in State laws.

III. METHODOLOGY

A. Process

The goal of developing our genetic privacy ontology is to identify diverse factors relevant to enforcing these laws in the United States. The applicable Federal law specific to genetic privacy is the GINA [27]. For State laws, the National Human Genome Research Institute maintains a Genome Statute and Legislation Database [28]. This database classifies the laws into the following categories:

- Employment Nondiscrimination
- Health Insurance Coverage
- Health Insurance Nondiscrimination
- Other Lines of Insurance Nondiscrimination
- Other Topics
- Privacy
- Research
- Use of Residual Newborn Screening Specimens

A search against all categories generated a list of over 400 individual state statues that were reviewed for their applicability. The focus was for statues with criteria that would impact a request to an EHR or similar repository. References to other statues within those on the search list

 ISBN: 978-1-61208-618-7

were followed when there was a potential for additional relevant use cases.

The next step in the process involved reviewing every relevant law for the specific terms and phrases associated with privacy protection. Statements and phrases related to the following super-classes (with two examples listed below for each item) were extracted:

- **Purpose**: What use case is being addressed? (law enforcement, treatment)
- **Subject**: Whose information is being protected? (individual, minor child, family member)
- **Requester Role**: what role is specified for individual making the request? (physician, genetic counselor)
- **Requester Organization**: What kind of organization does the requester represent? (insurance company, court)
- **Target of Request**: What kind of information or activity is protected? (genetic information, test results)
- **Pre-conditions**: What must be done before the information can be released? (obtain consent, approved by an institutional review board)
- **Post-conditions**: What must be done, or not done, once the information is provided? (non-discrimination, destroy after use)
- **Penalties**: How will any violations potentially be punished? (misdemeanor, fine)

Then, all super-classes were structured into relevant classes. For example, the Subject super-class was divided into the Individual, Immediate Family, Beneficiary, and Relative classes. The Relative class has additional subclasses for Blood Relative, Family Member, and Identical Brother. In order to ensure the appropriate coverage, similar terms were recorded in the detailed model (which is not presented here due to space constraints.) An example is that "Treatment" is used as the class name and is in the model, while "patient care" provides the same base meaning. Properties are added to the ontology solely based on the associated State law.

B. Exclusions

The expansive state database generated a comprehensive set of criteria for genetic privacy protection. Use cases not relevant to protecting genetic information in medical records were excluded from data elements analysis. For example, while there are State laws related to maintaining State DNA Databases for the criminal justice system, these laws were not evaluated after the first screening review. In addition, the search was not expanded to address Federal and State regulations as the basis of this guidance is derived from the associated laws. Finally, laws that provide generic protection to any component of protected health information and would be enforced across all information requests were not included. For example, while most State laws on genetic privacy are relatively recent and still being legislated, HIPAA restrictions have been in place since 1996 and are well established within the medical and insurance community [29].

IV. GENETIC PRIVACY ONTOLOGY

The Genetic Privacy Ontology as shown in Figure 1 is organized into four high-level components to reflect aspects of accessing medical records.

- **Requester** is information on the individual submitting the access request with their associated role and organization. The role and organization are linked with the purpose for a specific request. For example, a law may permit physician access to records for patient treatment at a hospital with a different set of conditions if the physician is participating in research at that facility.
- **Request** indicates characteristics of the person whose medical record is being accessed (subject), how the information will be used (purpose), what will be done with the information once received (action), and what information or activity is being requested (target).
- **Validation** provides conditions that must be addressed prior to information release (pre-conditions) and if a consent agreement is required with specific clauses to be included (consent).
- **Constraint** addresses limits placed on the use of the data (restrictions) and activities to be performed after the request is fulfilled (obligations).

This paper addresses the Requester and Request components as the most important aspects of enforcing the law. The laws vary widely in terms of which classes are specifically included and the amount of detail provided. As an example of a law with broad scope, the genetic information access law in Arkansas states "*Except as provided in (b) of this section … (1) a person may not collect a DNA sample from a person … unless the person has first obtained the informed and written consent of the person…"* followed by five specific purposes in section (b) where access is permitted.

A. Purpose

The Purpose super-class shown in Figure 2 provides the linchpin of genetic privacy protections. Every access to medical records must have a purpose (or reason for the access request). It is a violation of core security principles related to confidentiality to allow data access without a valid reason.

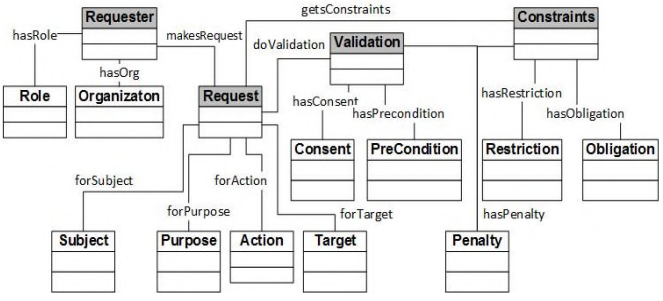

Figure 1. Genetic Privacy Ontology.

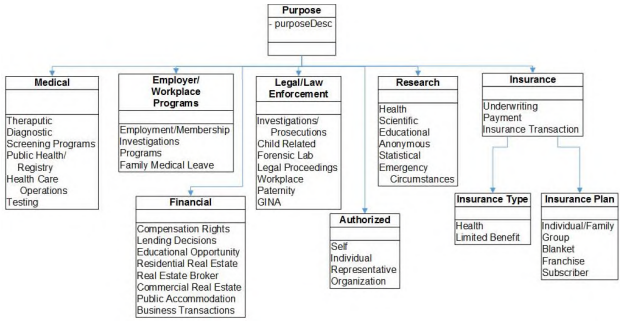

Figure 2. Purpose Super-Class.

The classes are:

- **Medical** with a focus on genetic-related activities plus access to genetic information for related efforts
- **Employer/Workplace Programs** includes labor organizations, apprenticeships, and licensing
- **Legal/Law Enforcement** for criminal, civil, court activities, compliance and related legal proceedings
- **Research** for health specific research, general scientific studies, educational programs, and access to deceased genetic information in an emergency situation
- **Insurance** for health plan underwriting, determining payments and other business transactions. There are two related subclasses for underwriting to determine the type of insurance being processed and the plan.
- **Financial** contains various financial transactions including whether a person is entitled to compensation for the use of their genetic material.
- **Authorized Person** allows access to records by people and organizations authorized in a consent agreement along with the individual themselves.

Many other classes have a direct relationship with a Purpose. For example, the Law Enforcement Purpose would only be applicable to Law Enforcement roles and other roles would be invalid. This linkage also applies to aspects of Organization and Target.

B. Action

During the full review of State laws, the need for an Action class as shown in Figure 3 became obvious to indicate how the interactions with the medical record will occur. The list follows the information lifecycle of a medical record from acquisition through use and destruction. These terms are extracted directly from the laws and each class contain lists of similar terms. For example, *Require* also addresses the terms Inspect, Compel, and Order.

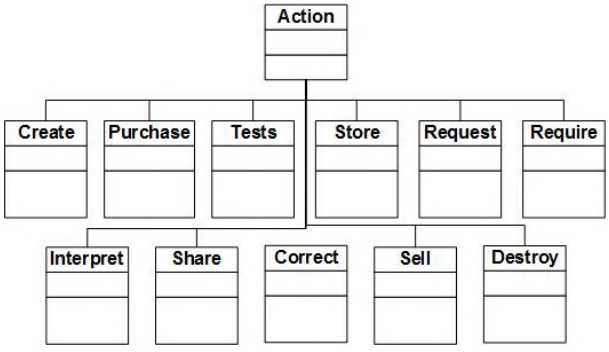

Figure 3. Action Super-Class.

Request and *Require* are separated to reflect the ability to deny a request for information as opposed to an inquiry that indicates a demand based on a compelling reason. For example, there are restrictions as to when insurance companies may request information and that the information may not be required as a condition of underwriting. In some cases, both terms are used as seen in the District of Columbia's law stating that "*A health benefit plan or health insurer shall not request or require an individual or the individual's family member to undergo a genetic test.*"

C. Subject

The Subject super-class in Figure 4 is larger than the immediate person in an access request. This broad definition is needed in order to accommodate laws with statements like the definition from a Delaware law, "*'Genetic information' means information about inherited genes or chromosomes, and of alterations thereof, whether obtained from an individual or family member…".* The Individual has subclasses with specific terms that map to purpose. For example, the Legal subclass has a law enforcement attribute in the full model for "*individual has been convicted of a felony*" to address a State law in New Mexico.

The age data field is not only a numeric value but a conditional codifying the decision-making capacity and age ranges. Some of the options beyond years of age include "*child born in the state*" and un-emancipated minor. A child can be minor child or also a reference to an adult child in the Family Member subclass. Fetus and embryos are called out specifically in some laws so they are articulated as a Subject subclass. Dependents are presented as a separate subclass, as these individuals are not necessarily a family member. The same criteria holds for Beneficiary as the person may not be directly related to the individual. This subclass is included as

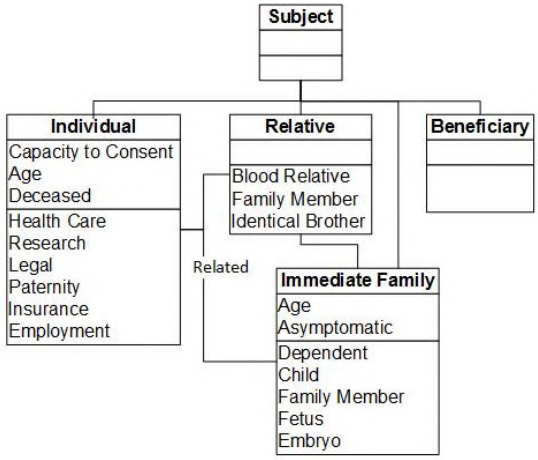

Figure 4. Subject Super-Class.

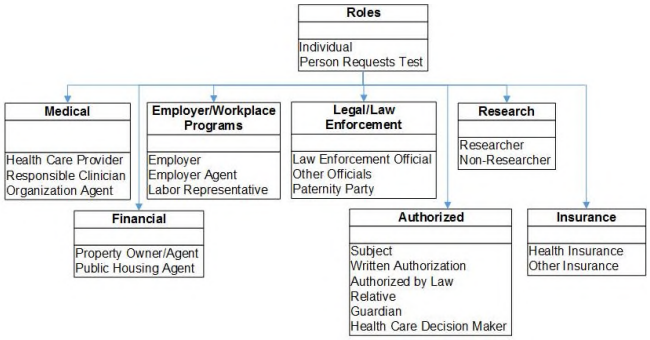

Figure 5. Role Super-Class.

Kentucky has a law that references the individual or their beneficiaries accessing genetic services.

D. Role

The majority of Roles in Figure 5 map to specific purposes and their use would be restricted to the associated purpose. There are general references to "*Individual*" accessing records so a broad subclass is needed for undefined people. Kentucky state law includes a reference to the person who orders a test on an infant or by the person registering the birth. The law is not clear that the request would be done by a health care provider so the category is separated.

Within an organization, the role becomes important for deciding on access. For example, a receptionist at a hospital does not have access to genetic information even though they work at a health care provider. Some terms are relevant to both individuals and organizations. For example, the term health care provider often means either entity.

E. Organization

Some terms that are typically associated with an individual may also be applicable to an Organization super-class which is provided in Figure 6. For example, the term *Person* can be a corporation in some states, such as defined in New Hampshire: "*Person includes a human being, an association or organization, a trust, corporation, and partnership*." The phrase "*Health Care Provider*" is also an organization in addition to a specific person/role. The use of subclasses with the same name as the Purpose super-class indicates a match where there are restrictions associated with the organization (and hence role). Therefore, a Research Organization would be limited to using Research Roles and Purposes for a valid combination.

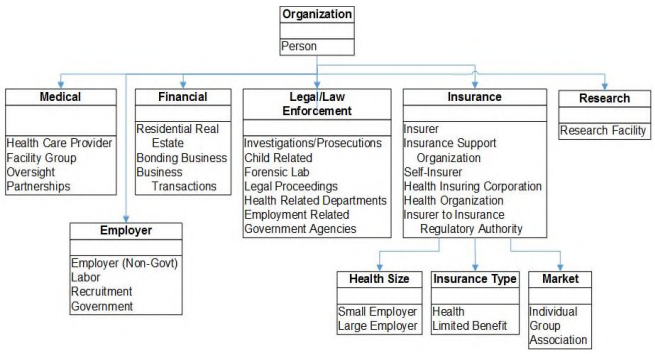

Figure 6. Organization Super-Class.

F. Target

The Target super-class in Figure 7 addresses the specific item being addressed in the law and encompasses more than genetic information.

- **Physical Specimens** are included as genetic material is derived from these sources and thus have specific access restrictions.
- **Record** includes all the information, data and audit records within an individual's medical records. Numerous states have restrictions not only on the results of genetic tests and activities, but also on whether a request was made and/or denied by an individual or family member. If a record has been de-identified, different handling is indicated in some states.
- **Organization** is included as some laws incorporate who is the custodian or holder of the records being accessed.
- **Health Status Information** (also called "health status related factors" and other phrases) is generally defined as including Health status, Medical condition (including both physical and mental illness), Claims experience, Receipt of health care, Medical history, Genetic information, Evidence of insurability including conditions arising out of domestic violence, and Disability. However, in some states genetic information is explicitly excluded as health status information.
- **Genetic Information** includes all the related subclasses. The state of Washington recently included genetic information as a biometric identifier so a state list is included.
- **Family Member** and their Genetic Information is often included in the scope of the individual's genetic information.
- **Research** addresses genetic information obtained in this purpose along with any genetic services obtained in association with the research. (This linkage is specifically called out.)
- **Genetic Services** is for those areas targeting genetic-

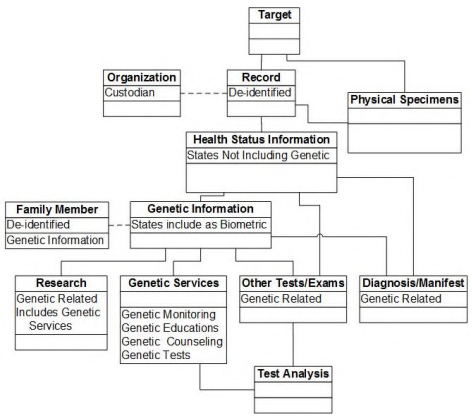

Figure 7. Target Super-Class.

related activities plus those tests performed specifically to identify genetic characteristics. The test results associated with these tests are also covered under the umbrella of protected genetic information.

- **Other Test/Exams** addresses medical procedures performed for reasons other than genetic services but the resulting information is genetic-related.
- **Diagnosis/Manifest** addresses those situations that indicate underlying genetic conditions not found directly by genetic services.

V. IMPLEMENTATION

Our previous prototype implemented a three-layer architecture for enforcing genetic information release criteria as seen in Figure 8. At the top layer, a workflow developed in Yet Another Workflow Language (YAWL) [30] orchestrates the information gathering on the Requester and Request, invokes the Consent Service layer, displays the access request decision (permit or deny) and gathers electronic signatures to enforce the Validations and Constraints. The Consent Service Layer uses Java code to obtain the information from the workflow, populate the ontology instances in Protégé, invoke the DL Reasoner, use the Rules Hierarchy Algorithm to combine the Federal, State and Local decisions into an overall final result, and populate the workflow variables with the results for display and action by the end user. The ontology itself in implemented in Protégé and the laws are encoded using Semantic Web Rule Language (SWRL) [31].

Our previous papers [32][33] provide extensive information on the prototype operation and detailed use cases. In this Section we provide targeted examples based on the purpose-focused ontology.

A. Related Organization

In New Mexico, genetic information access is allowed without patient consent *"(1) to identify an individual in the course of a criminal investigation by a law enforcement agency"*. The corresponding SWRL rule for this law is:

Rule: makesRequest(?r, ?req), inState(?req, "NM"), forResource(?req, ?resource), isGeneticResult(?resource, true), includesIdentity(?resource, true), forPurpose(?req, ?pur), isInvestigation(?pur, true), hasOrganizaton(?r, ?org), isLawEnforcement (?org, true), hasResponse(?req, ?resst), responseLevel(?resst, "State")→ isAllowed(?resst, true), canOverride(?resst, false), decisionSource(?resst, "NM LAW 24-21-3.C"),, hasRule(?resst, 3105)

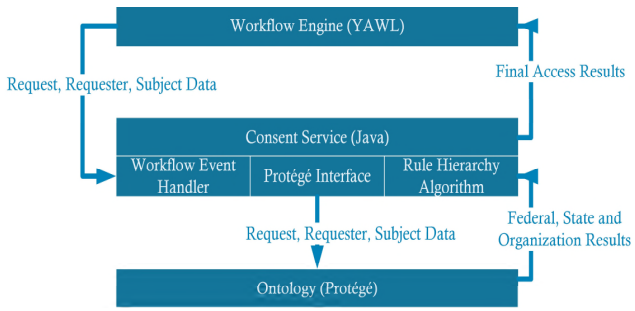

Figure 8. Prototype Architecture.

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 Purpose for the Request
- ?resource is for the "GeneticTestResults" part of the medical record
- ?org is the Organization f the Requester
- ?resst is the State Response object that is associated with the Request.

These SWRL statements are explained in Table I.

TABLE 1. SAMPLE PURPOSE-FOCUSED RULE

SWRL Statement	***Explanation***
makesRequest(?r, ?req)	Links Requester for the Request
inState(?req, "NM")	Request is for New Mexico
forResource(?req, ?resource)	Links Request with the Resource
isGeneticResult(?resource, true	Restricts the rule to a Resource that is identified as a genetic test results
includesIdentity(?resource , true)	Restricts the rule to Resources that are used to confirm identity
forPurpose(?req, ?pur)	Links Request with Purpose
hasOrganizaton(?r, ?org)	Links Organization with the Requester
isLawEnforcement (?org, true)	Confirms the Organization is a Law Enforcement Agency
hasResponse(?req, ?resst)	Links the Request with a Response to store answer
responseLevel(?resst, "State")	Gets the Response for the State level answers
-> isAllowed(?resst, true)	Sets the State response to access is allowed
canOverride(?resst, false)	Sets the State Response to not allow organization override
decisionSource(?resst," NM LAW 24-21-3.C ")	Sets the State response to reflect the decision source as state law
hasRule(?resst, 3105)	Sets the rule number to 3105 for reference

Boolean attributes are used in the ontology to simplify the evaluation of specific conditions. For example, *isLawEnforcement* allows any organization that meets the criteria to be provided access in relation to the *isInvestigation* attribute for Law Enforcement purposes. In numerous laws related to law enforcement, the statement specifically calls out using the genetic information for identifying a person. Therefore, an *includesIdentity* attribute is associated with the genetic information resources to exclude any that are medically focused. The Boolean attributes enhance the flexibility of the ontology implementation.

B. Broad Statements

Some states have broad statements that all uses for genetic information are denied (or permitted) except as outlined in a specific list. This scenario is addressed by assigning state-specific attributes to the *Purpose* class. Then the allowed *Purpose* instances are set to true and all other instances are set to false.

For example, in Alaska, consent is required to collect DNA sample, perform DNA analysis, retain DNA sample or results, or disclose results except for the following cases:

- Public Safety DNA database
- Law Enforcement purpose
- Determining Paternity
- Screen Newborns
- Emergency Medical Treatment

An attribute is added to *Purpose* for *isAKConsentRequired* which can be set to true for these specific instances. (The official state abbreviation for Alaska is AK.) Within the *Medical* class, most instances under the *Therapeutic* subclass would have attribute set to true with only Emergency Medical Treatment set to false. A sample SWRL rule that would be invoked for Emergency Medical Treatment is as follows:

makesRequest(?r, ?req), inState(?req, "AK"), forResource(?req, ?resource), isGeneticResult(?resource, true), forPurpose(?req, ?pur), isAKConsentRequired(?pur, false), hasResponse(?req, ?resst), responseLevel(?resst, "State") -> isAllowed(?resst, true), canOverride(?resst, false), decisionSource(?resst, "AK LAW 18.13.010"), hasRule(?resst, 23)

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 Purpose that is associated with the Request
- **?resource** is for the "GeneticTestResults" part of the medical record
- **?resst** is the State Response object that is associated with the Request.

These SWRL statements are explained in Table II.

TABLE II. SAMPLE BROAD STATEMENT RULE – NO CONSENT

SWRL Statement	***Explanation***
makesRequest(?r, ?req)	Links Requester for the Request
inState(?req, "AK")	Request is for Alaska
forResource(?req, ?resource)	Links Request with the Resource
isGeneticResult(?resource, true	Restricts the rule to a Resource that is identified as a genetic test results
isAKConsentRequired(?pur, false)	Restricts the rule to Purposes that do not require consent
forPurpose(?req, ?pur)	Links Request with 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
-> isAllowed(?resst, true)	Sets the State response to access is allowed
canOverride(?resst, false)	Sets the State Response to not allow override by organization
decisionSource(?resst, "AK LAW 18.13.010")	Sets the State response to reflect the decision source as State law
hasRule(?resst, 23)	Sets the rule number to 23 for reference

The corollary rule that would be invoked for any other Medical purpose is as follows:

makesRequest(?r, ?req), inState(?req, "AK"), forResource(?req, ?resource), isGeneticResult(?resource, true), forPurpose(?req, ?pur), isAKConsentRequired(?pur, true), hasResponse(?req, ?resst), responseLevel(?resst, "State"), oblName(?pre, "ConsentRequired"), clauseName(?clause, "AKGeneticConsent") -> isAllowed(?resst, true), canOverride(?resst, true), decisionSource(?resst, "AK LAW 18.13.010"), hasPreCondition(?resst, ?pre), hasClause(?resst, ?clause), hasRule(?resst, 21)

The additional arguments from the previous example are:

- **?pre** is for a specific the Pre-Condition
- **?clause** is for the text in the designated consent clause

 ISBN: 978-1-61208-618-7

The SWRL statements that are different than the previous rule are explained in Table III.

A side effect of these rules is that Alaska state law does not define any situation where access is denied as long as consent is obtained.

TABLE III. SAMPLE BROAD STATEMENT RULE –CONSENT REQUIRED

SWRL Statement	***Explanation***
isAKConsentRequired(?pur, true)	Restricts the rule to Purposes that do require consent
oblName(?pre, "ConsentRequired")	Gets the obligation that indicates consent is required
clauseName(?clause, "AKGeneticConsent")	Gets the specific consent clause required in Alaska for access
hasPreCondition(?resst, ?pre),	Sets the State response to include the Consent Required condition
hasClause(?resst, ?clause),	Sets the State response to include the specific Consent Clause
hasRule(?resst, 21)	Sets the rule number to 23 for reference

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] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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: 04-Feb-2018].

[10] 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: 04-Feb-2018].

[11] "State and Federal Consent Laws Affecting Interstate Health Information Exchange." [Online]. Available: https://www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-health-publications/col2-content/main-content-list/state-and-federal-consent-laws-a.html. [Accessed: 04-Feb-2018].

[12] "Enabling Document Sharing Using IHE Profiles - IHE Wiki." [Online]. Available: http://wiki.ihe.net/index.php/Enabling_Document_Sharing_Using_IHE_Profiles. [Accessed: 04-Feb-2018].

[13] "Basic Patient Privacy Consents - IHE Wiki." [Online]. Available: http://wiki.ihe.net/index.php/Basic_Patient_Privacy_Consents. [Accessed: 04-Feb-2018].

[14] 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.

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

[16] "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.

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

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

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

[20] J. M. Oliver et al., "Balancing the Risks and Benefits of Genomic Data Sharing: Genome Research Participants' Perspectives," Public Health Genomics, vol. 15, no. 2, pp. 106–114, 2012.

 ISBN: 978-1-61208-618-7

[21] T. Haeusermann et al., “Open sharing of genomic data: Who does it and why?,” PLoS ONE, vol. 12, no. 5, p. e0177158, May 2017.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] Genetic Information Nondiscrimination Act of 2008. 2008.

[28] “Genome Statute and Legislation Database,” National Human Genome Research Institute (NHGRI). [Online]. Available: https://www.genome.gov/. [Accessed: 04-Feb-2018].

[29] Health Insurance Portability and Accountability Act of 1996. 1996.

[30] 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.

[31] H. Knublauch, R. W. Fergerson, N. F. Noy, and M. A. Musen, “The Protégé OWL Plugin: An Open Development Environment for Semantic Web Applications,” in The Semantic Web – ISWC 2004, 2004, pp. 229–243.

[32] 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.

[33] 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.

 ISBN: 978-1-61208-618-7