Sharing Data under Genetic Privacy Laws

Michael Reep*, Bo Yu*, Duminda Wijesekera*, Paulo Costa †
* Department of Computer Science, George Mason University, Fairfax, VA, USA
mreep@gmu.edu, byu3@gmu.edu, dwijesek@gmu.edu
† Department of Systems Engineering and Operations Research, George Mason University, Fairfax, VA, USA
pcosta@gmu.edu

***Abstract*— Clinical medical practice and biomedical research utilize genetic information for specific purposes. Irrespective of the purpose of obtaining genetic material, methodologies for protecting the privacy of patients/donors in both clinical and research settings have not kept pace with rapid genetic advances. When the usage of genetic information is not predicated on the latest laws and policies, the result places all-important patient/donor privacy at risk. Some methodologies err on the side of overly stringent policies that may inhibit research and open-ended diagnostic activity, whereas an opposite approach advocates a high-degree of openness that can jeopardize patient privacy, identifying patient relatives and erode the doctor-patient privilege. As a solution, we present a unique approach that is based on the premise that acceptable clinical treatment regimens are captured in workflows used by caregivers and researchers and therefore their associated purpose can be extracted from these workflows. We combine these purposes with applicable consents (derived from applicable laws) to ascertain the releasability of genetic information. Given that federal, state and institutional laws govern the use, retention and sharing of genetic information, we create a three-level rule hierarchy to apply the laws to a request and auto-generate consents prior to releasing. We prototype our system using open source tools, while ensuring that the results can be added to existing Electronic Medical Records (EMR) systems.**

Keywords—genetic privacy, electronic medical records, ontology, health care, genomic medicine, SWRL

I. INTRODUCTION

Genetic studies match genotypic and phenotypic data to associate genetic markers with onset of diseases [1]. Studies have shown that preventive care costs significantly less than treatment upon disease onset and diagnosis [2, 3]. Furthermore, rapid advancement of genetic research continues to lengthen the list of predictable diseases. Examples include genetic mutations causing some breast cancers (BRC-1 and BRC-2), ovarian cancer, sickle cell anemia, β-thalassemia, left ventricular noncompaction cardiomyopathy and Alzheimer's disease. However, both research and clinical use of genetic information entail privacy challenges that differ from usage of other medical data in following ways:

* Ethics - Privacy of genetic data differs from traditional medical information privacy. For example, protecting patients' private information (e.g., Protected Health Information - PHI) is an important medical ethics and legal obligation. Data for genotype-phenotype matching can be used to stigmatize or discriminate against genetic relatives of a donor, so the dangers of its exposure must be carefully weighed against the benefits of its use [1, 4, 5]. There is an ongoing ethical debate between the two different schools of thought, one in which the donor gives open consent for using his/her data vs. the other that advocates explicit purpose-based consent [6].

* Legal Issues - Due to the unusual situation of being able to expose relative's genetic composition, genetic privacy has been proposed as categorical privacy that differs from traditional individual-centered concepts of privacy in literature [7]. Federal (HIPAA and GINA) [8, 9], state laws and institutional polices provide the legal framework for the sharing of genetic information. Furthermore, genetic privacy laws vary from state-to-state and may be inconsistent with, or more or less stringent than, federal regulations.

* Social Implications - Societal views are often reflected in law and/or organizational policies, so their implications are likely inextricably intertwined with laws and policy governing genetic privacy and what constitutes informed consent.

As a solution, we provide an encompassing framework consisting of workflow-enforced genetic privacy as well as biomedical consent management, consistent with state and federal genetic privacy laws such as statute, regulation and precedent. Following this Introduction, Section 2 addresses related work; Section 3 reviews the prototype design and ontology,

Section 4 describes the implementation of our genetic services workflow that enforces appropriate informed consent based on applicable law to achieve genetic privacy; and, finally, Section 5 presents conclusions.

II. Related Work

Many researchers have suggested adopting traditional information protecting methodologies to protect patients' confidentiality. Yet, this might not be effective due to the uniqueness of being traceable to an individual or group of individuals [10, 11]. After all, some genetic information of an individual may not only precisely identify him/her as high risk of certain hereditary disease(s), but also indicate that his/her relatives have the same risks due to a heritable gene.

Prince et. al. describe three practical genetic counseling cases that illustrate genetic discrimination [12]. The fundamental covenant of protecting patient privacy is embodied in patient-doctor privilege. Conversely, many scholars believe *genetic information is essentially familial in nature and is referred to as the Genetic Information is Familial Thesis (GIFT)* [13], since sharing such information will benefit related groups of individuals. Some countries have regulations to enforce sharing such information among family members [14, 15]. However, many publications discuss and debate the familial approach, with their authors advocating the view that humans possess the rights of privacy and to protect those that *do not want to know* [13, 16]. Conversely, rapid innovations in genetic research require wide accessibility to many genetic databases. The idea of open access in the field of genomic research is expressed in the Bermuda Principles and the Fort Lauderdale Agreement, which has been applied in North America and in the UK for funded research [17]. Genetic research typically requires additional metadata with genetic data sets, such as demographic details family relationships, medical history, etc. These metadata elements can be exploited for tracing an individual's identity.

In general medicine, an informed consent, especially informed privacy consent, provides the proper opportunity and knowledge for patients and research participants to understand and decide how the medical community can use and share their identifiable medical information. Analogously, informed consent tailored for genetic research, clinical usage and counseling constitutes a strong basis for ensuring appropriate genetic privacy. Some genetic medical practices and biomedical research are performed without obtaining appropriate informed consent such as enticing participants in a study without obtaining the proper informed consent. To address this issue, some researchers advocate different methodologies such as using highly-stringent policies to maintain patient confidentiality, but this approach potentially risks limiting scientific innovation [18]. Yet, other researchers have proposed a new, open-consent model for medical and scientific genetic research [7] or open-access policies for genetic data sharing [19]. As the underlying predicate for us undertaking this effort, we proposed a prototype system capable of automatically generating or obtaining appropriate informed consent forms for genetic data sharing under various situations.

EMRs play a vital role of sharing medical information among participating actors based on their usage scenarios. Using EMRs for genetic services present a unique set of challenges [20]. Belmont et al. highlighted the privacy, ethical and legal issues of handling genetic data in EMRs [21]. Scheuner et al. conducted a case study to validate if current EMR systems meet genetic information needs [22]. This study shows an overall lack of support for functionality, structure, and tools for clinical genetic practice. A more recent study of the state of EMRs supporting genomics for personalized medicine identifies structure of data as a challenge [23]. Therefore, it is necessary to implement an informed consent management system in current EMRs.

Some researchers suggested that the legislation for generating and using genetic information properly is pivotal to improving genetic privacy [24]. In 2013, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [8] Omnibus Rule included genetic information as PHI to be regulated under the privacy portion of HIPAA.

Nonetheless, states may have different definition of genetic information. The combination of Federal privacy laws along with the various state laws form a fragmented regulatory and statutory landscape for permissible information sharing and consent management. To be valid, informed consents for genetic privacy must comply with these laws and regulations. Indeed, significant regulatory gaps create additional burdens in providing automated ways to obtain and generate information consent in EMRs.

III. System Design

We developed a functioning prototype that addresses the various aspects for an automated and integrated informed genetic information consent system. The prototype brings together the data gathered during interactions with the medical provider with the applicable laws, regulations and policies to address the privacy issues specific to genetic information. There are three components of the prototype as shown in Fig. 1:

- Workflow to gather the information, display the outcome and obtain acceptance from the user of the results and any pre/post conditions for using the data.
- A ontological rule-base that takes the data from the workflow, evaluates the applicable laws, determines prerequisites (such as consents and obligations), and decides on the releasability of genetic data.
- A consent service that interacts with the workflow engine and ontology to pass data back and forth. The service includes the Rule Hierarchy Algorithm which combines the outcomes from the three levels (Federal, State and Organization) and provides a final result for permitting or denying access. The outcome includes the consolidated list of conditions for all three levels. For example, the list of consent clauses required by both the Federal regulations and organizational policies.

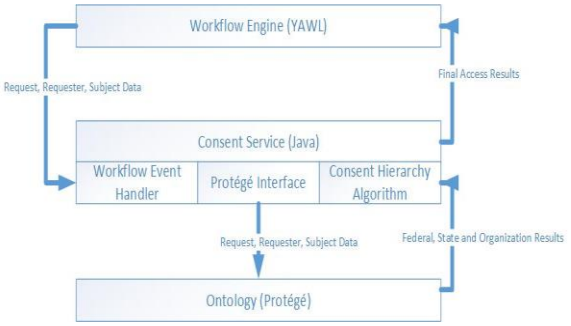

Fig.1. Prototype Components

The first component of implementing the genetic privacy enforcement is to gather the required information through the workflow. As the usage scenario is executed (under the workflow engine) the meta-data required to determine the releasability of data is gathered and passed to the consent service. The consent service then creates the objects and relationships in the ontology for evaluation by the reasoner. Next the service retrieves the results and calls our 3-level rule hierarchical algorithm. The service determines if access is permitted and passes the access results back to the workflow engine. The acknowledgment steps in the workflow display the results along with the decision source (specific law or regulation referenced), the consent clauses, obligations to be enforced for information released, and the specific rules used in the ontology to generate the answer.

To support the consent service, we developed an ontology to capture the various aspects of enforcing privacy laws and policies. As seen in the Fig. 2 the prototype requires four related data items.

- Requester: the person making the request to access the medical information including their role, associations with a specific organization, and information about this organization,
- Request: details on the purpose for requesting the information, and where the information will be used. The four purposes applicable to genetic information are disclosure, research, testing and treatment. The prototype currently implements the information disclosure component with the applicable specific instances for Self-Request by the Patient, Law Enforcement, etc.
- Response: the results of the reasoner applying the appropriate rules along with a list of any obligations that must be enforced by the EMR and specific consent clauses that are needed for the associated approvals. (A subclass for

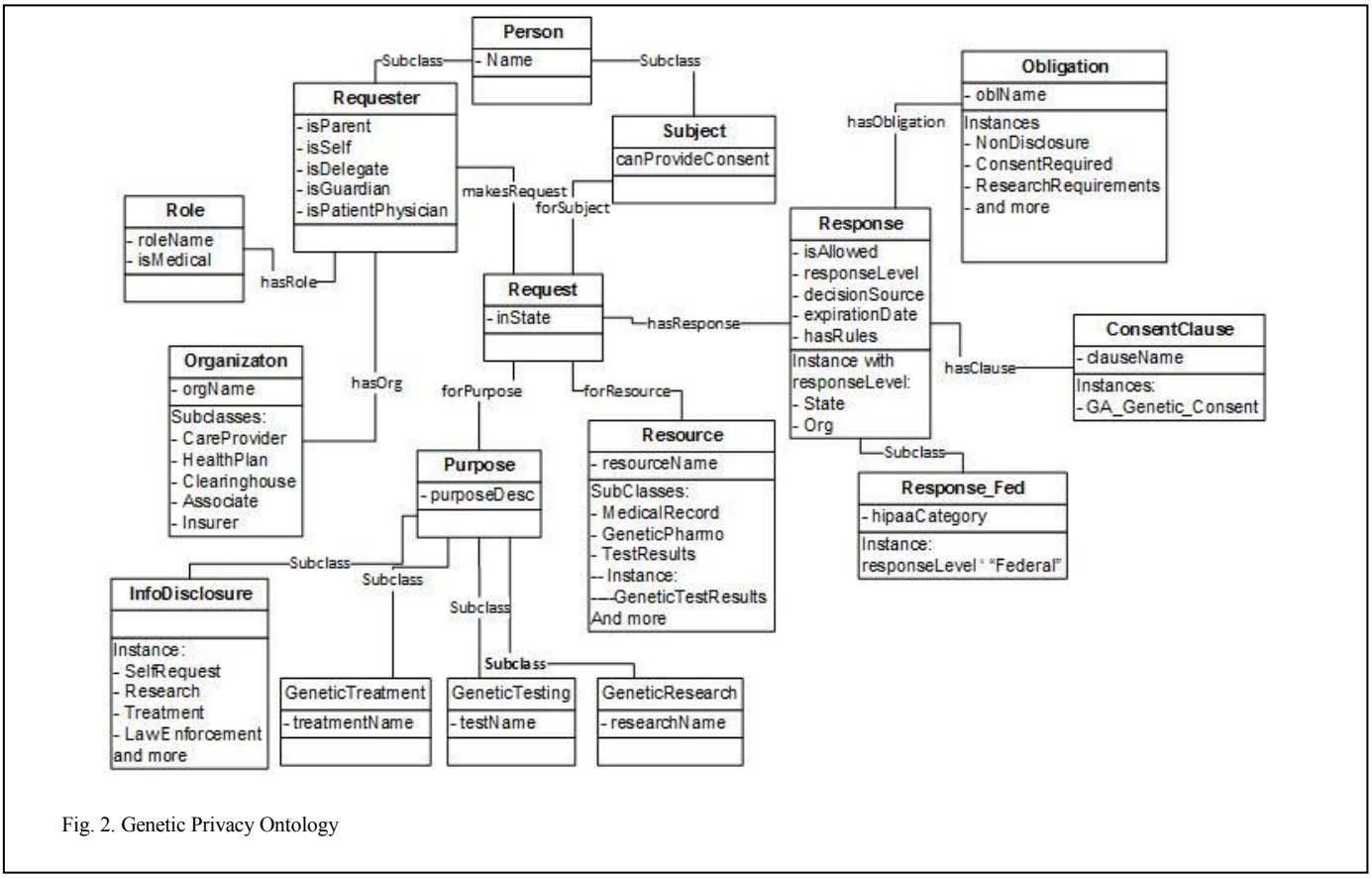

Fig. 2. Genetic Privacy Ontology

Federal Responses allows information about HIPAA-specific requirements to be gathered.)

- Resource: the part of the electronic medical record being requested along with information about the subject (or patient). The Resource instances can be used to categorize detailed levels of rules such as enforcing restrictions to specific parts of the genome that can be used to identify individuals or grant permission to components used in genomic medicine.

The ontology does not need to contain all the information from the EMR because the current focus is on rules implementation. Many entities in the ontology provide reference information such as the organizational meta-data or a list of specific Consent Clauses that are not described presently.

The Rule Hierarchy Algorithm evaluates the interactions between Federal and State laws, regulations and institutional policies. The access evaluation is done at each level (Federal, State and Organization) in the hierarchy that is applicable for the specific access request. By definition, Federal laws are at the top of the hierarchy, followed by State laws, and then organizational policies. The hierarchy algorithm dictates how conflicts between laws and policies can be resolved based the decisions made at each level.

In order to address these potential conflicts, Federal and State laws have an override flag associated with them in the ontology to indicate whether lower level rules can change the answer. If two levels come to the same conclusion (both permit access), the supplemental clauses and obligations are combined into one complete response. For example, HIPAA permits access to medical records for treatment. In Georgia, there are additional obligations and consent requirements when the resource being accessed is from genetic testing.

The Response structure allows both sets of answers to be passed back to the EMR for evaluation and execution. However, if the results were different, the previous answers are discarded in favor of the lower level requirements in order to resolve the inconsistency. For example, if Federal law permitted access and allowed an override to the Permit decision,

the organizational policy may come to a different conclusion and set the response to Deny.

The Rule Hierarchy Algorithm follows:

```
INIT {resAns, resObl, resDec, resCl, resRule} to {fedAns,
fedObl, fedDec, fedCl, fedRule}                          (1)
IF fedOver = true THEN                                   (2)
        IF stAns <> null THEN                            (3)
                IF stAns = fedAns THEN                   (4)
                        resAns = resAns + stAns          (5)
                        resObl = resObl + stObl          (6)
                        resAns = resDec + stDec          (7)
                        resAns = resCl + stCl            (8)
                        resAns = resRule + stRul         (9)
                ELSE                                     (10)
                        resAns = stAns                   (11)
                        resObl = stObl                   (12)
                        resAns = stDec                   (13)
                        resAns = stCl                    (14)
                        resAns = stRule                  (15)
                END IF                                   (16)
        END IF                                           (17)
        IF (orgAns <> null) AND (((stAns <> null) AND
(stOver = true)) OR (stAns = null))) THEN                (18)

                IF orgAns = resAns THEN                  (19)
                        resAns = resAns + orgAns         (20)
                        resObl = resObl + orgObl         (21)
                        resAns = resDec + orgDec         (22)
                        resAns = resCl + orgCl           (23)
                        resAns = resRule + orgRul        (24)
                ELSE                                     (25)
                        resAns = orgAns                  (26)
                        resObl = orgObl                  (27)
                        resAns = orgDec                  (28)
                        resAns = orgCl                   (29)
                        resAns = orgRule                 (30)
                END IF                                   (31)
        END IF                                           (32)
END IF                                                   (33)

RETURN resAns, resObl, resDec, resCl, resRule            (34)
```

In (1) the Result variables for the Answer, Obligations, Decision Source, Clauses and Rules are initialized to the corresponding federal variables, which were retrieved from Protégé. In (2) the Federal Override variable is evaluated to determine whether other rules are to be evaluated. If so, (3) checks for State answer existing and, if found, (4) determines if the Federal and State answer match. Lines (5)-(9) adds the State variables to the Result variables when the Federal and State match while (11)-(15) set the Results variables to the State results when there is no match.

For the Organization level, Line (18) determines if there is an Organization result and whether there is a State result with a State Override flag set to true or there is no State answer. If (18) is true, then (20)-(24) adds the Organization variables to the Result variables, while (26)-(30) set the Results variables to the Organization results. At the end of processing (34) the Results variables are passed back to the workflow via the YAWL API.

IV. System Implementation

The prototype was developed using the YAWL (Yet Another Workflow Language) workflow engine with Java classes that respond to the YAWL event handlers to trigger the ontology processing and Rule Hierarchy Algorithm. As seen in Fig. 3, the consent workflow gathers additional information regarding aspects of the tasks being performed, the requester and the subject before executing a call to the Consent Service in the "Check Consent" step. A final step is provided for validating that the results are acknowledged before returning the response to the associated EMR.

The first YAWL screen shown in Fig. 4 is for the "Get Request Information" step in the workflow process to describe why the request is needed, what part of the medical record is to be accessed, in what state the action is being performed and, for research purposes, whether the request is for an individual or group. Each of the three Get steps have a similar screen. The "AckPermit" screen in Fig. 4 shows the results, pre and post-conditions for using the information, and an input box to enter in acceptance. For an implementation such as an integration with the OpenMRS, these YAWL screens will be replaced with others that will be embedded in the EMR product.

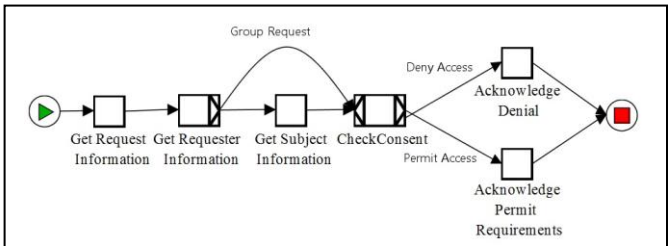

Fig.3. Genetic Privacy Workflow

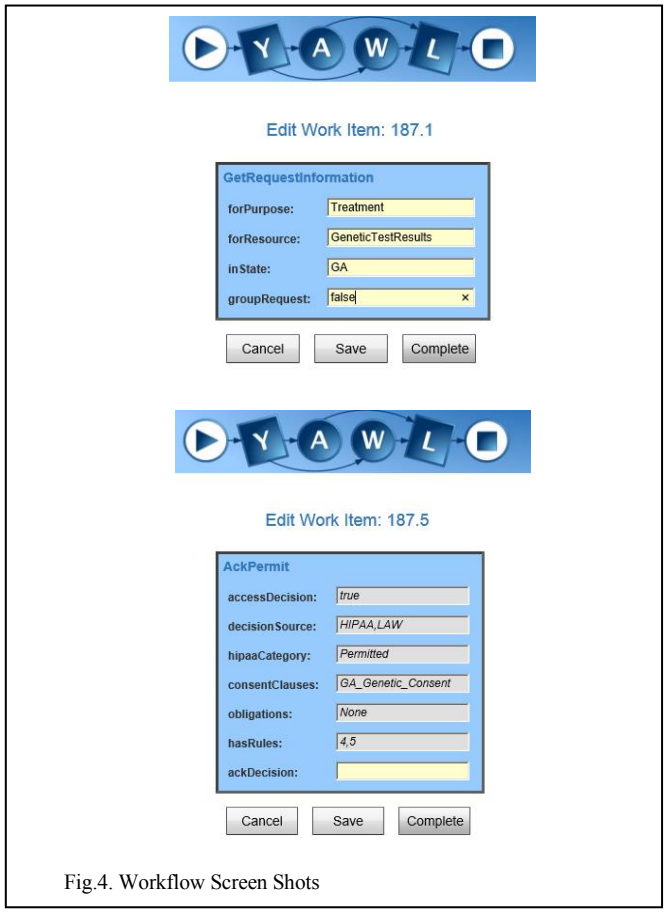

Fig.4. Workflow Screen Shots

Once the consent service is called and the results generated, the latter are displayed for validation by the user. EMR integration will allow some of the tasks, such as generating consent letters, to be implemented and enforced within the product. The Consent Service serves as the integration engine between the workflow/EMR and the ontology. The Java-based Consent Service is triggered by a YAWL event handler on the Check Consent workflow step. The service then gathers all the data from the workflow entries to create and populate the ontology instances including the data and object properties. The object properties link the instances such as establishing the makesRequest relationship between the Requester instance and the Request. Once the data has been populated in the ontology, the reasoner generates the responses and stores the information. The service extracts the response information for evaluation using the Rule Hierarchy Algorithm.

The ontology is implemented using the Protégé platform with the laws and regulations (Federal and State) plus the organization policies enforced via SWRL rules and the Pellet reasoner. The predicate of each rule uses the Request instance with the associated object properties to gather additional information on the Requester, Subject, Purpose and the Resource. (These values were all gathered and populated by the workflow and consent service.) For example, the Request instance is linked in the ontology to the associated Purpose using the hasPurpose object property. The appropriate Response instance (Federal, State or Organization) stores the outcome of the rule regarding whether access is permitted or denied, whether an override is allowed (Federal and State), the HIPAA Category (Federal), the specific law or policy that generated the result, any appropriate obligations and clauses (via hasObligation and hasClause object properties), and a rule number that maps to the SWRL rule.

An example of the implementation is a request to access the Genetic Test Results resource for the Treatment purpose in Georgia. As seen in Fig. 5, there are two different aspects to the Request: establishing relationships to other objects with relevant information and specific data properties for this request. The first object property assertion links the request to the part of the medical record the requester would like to access. The next three object assertions link to response objects that will hold the access permission (permit/deny) and other information associated with the rules for each level (Organization, State and Federal). The next two object assertions link indicate which person is the subject of the request (generally a patient) and the purpose for accessing the medical record. The data

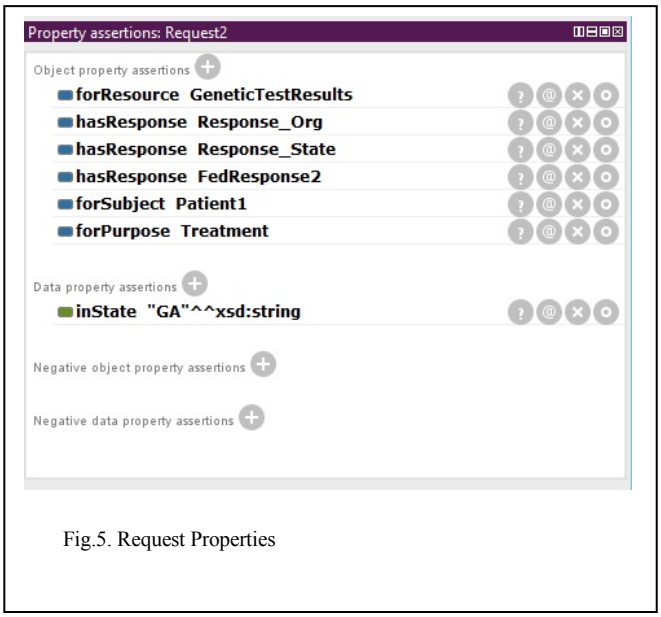

Fig.5. Request Properties

assertion states that the request is being made in the state of Georgia ("GA").

The first SWRL rule below as seen in Protégé addresses the Federal law for access under the Treatment purpose.

makesRequest(?r, ?req), forPurpose(?req, ?pur), purposeDesc(?pur, "Treatment"), hasResponse(?req, ?res), responseLevel(?res, "Federal") -> isAllowed(?res, true), canOverride(?res, true), hipaaCategory(?res, "Permitted"), decisionSource(?res, "HIPAA"), hasRule(?res, 4)

In this example,

- ?r is for the Requester for the Request
- ?pur is the Purpose for "Treatment"
- ?req is the Request being made for the Federal Level with the Treatment Purpose
- ?res is the Federal Response that is associated with the Request.

The explanation for each of these SWRL statements is provided in Table I.

TABLE I. SAMPLE FEDERAL RULE

SWRL Statement	***Explanation***
makesRequest(?r, ?req)	Links Requester to the Request
forPurpose(?req, ?pur)	Links Request with the Purpose
purposeDesc(?pur, "Treatment")	Restricts the rule to only execute for the Treatment purpose description
hasResponse(?req, ?res)	Links the Request with a Response to store answer
responseLevel(?res, "Federal")	Gets the Response for Federal level
-> isAllowed(?res, true)	Sets access to true in Response
canOverride(?res, true)	Sets override to true
hipaaCategory(?res, "Permitted")	Sets HIPAA category to Permitted
decisionSource(?res, "HIPAA")	Sets the decision source as HIPAA
hasRule(?res, 4)	Sets the rule number to 4

When the Pellet reasoner finds a set of instances that matches the Treatment and Federal conditions, the rule is executed and the ?res data properties populated with the values indicated. As seen in Fig. 6, the Federal Response is updated with the final values.

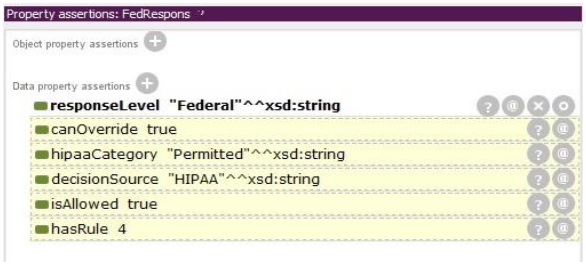

Fig.6. Federal Response

The next part of the example below shows the SWRL rule for the State response, the SWLR statements explained in Table II, and the response in Fig. 7. In the SWRL rule, the predicate sets the location as Georgia and that the rule can be executed if the Federal response allows an Override. The predicate also retrieves an additional obligation for a Consent Agreement and the agreement must have text specific to Georgia. The State response then is set to allow access with no override and information that the decision was based on Georgia Law. The response is linked to an obligation for a Consent Agreement and the consent clause with text specific to Georgia.

isSelf(?r, false), makesRequest(?r, ?req), inState(?req, "GA"), forResource(?req, ?resource), forPurpose(?req, ?pur), purposeDesc(?pur, "Treatment"), resourceName(?resource, "GeneticTestResults"), hasResponse(?req, ?res), responseLevel(?res, "Federal"), canOverride(?res, true), hasResponse(?req, ?resst), responseLevel(?resst, "State"), oblName(?obl, "ConsentRequired"), clauseName(?clause, "GAGeneticConsent") -> isAllowed(?resst, true), canOverride(?resst, false), decisionSource(?resst, "GA_LAW"), hasObligation(?resst, ?obl), hasClause(?resst, ?clause), hasRule(?resst, 5)

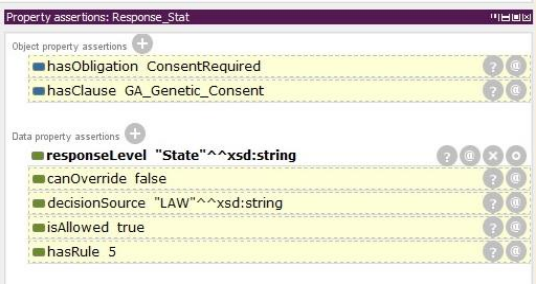

Fig.7. State Response

In the State example, the additional instances used are:

- ?resource is for the "GeneticTestResults" part of the medical record
- ?r is the Requester associated with the Request
- ?obl has the Obligation that ConsentRequired must be obtained for this request
- ?clause indicates the consent agreement for the patient must include the GAGeneticConsent clause
- ?resst is the State response associated with the Request

The explanation for each of these SWRL statements is provided in Table II.

TABLE II. SAMPLE STATE RULE

SWRL Statement	*Explanation*
isSelf(?r, false),)	Verifies Requester is not the subject
makesRequest(?r, ?req),	Links Requester for the Request
inState(?req, "GA"),	Verifies Request is for Georgia
forResource(?req, ?resource)	Links Request with the Resource
forPurpose(?req, ?pur)	Links Request with the Purpose
purposeDesc(?pur, "Treatment"),	Restricts the rule to only execute for the Treatment purpose description
resourceName(?resource, "GeneticTestResults")	Verifies Resource request is for the Genetic Test Results
hasResponse(?req, ?res)	Links the Request with a Response to check previous rule results
responseLevel(?res, "Federal")	Limits the previous Response to Federal
canOverride(?res, true)	Verifies the Federal rule allows overrides
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, "ConsentRequired")	Gets the Obligation for Consent Required
clauseName(?clause, "GAGeneticConsent")	Gets the Clause for Consent Required
-> 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, "GA_LAW")	Sets the State response to reflect the decision source as state law
hasObligation(?resst, ?obl)	Links the retrieved Obligation with the State response
hasClause(?resst, ?clause)	Links the retrieved Clause with the State response
hasRule(?resst, 5)	Sets the rule number to 5 for reference

When the Pellet reasoner finds a set of instances that matches the Treatment for someone besides the Requester in GA for GeneticTestResults and the Federal response has Override set to True, the rule is executed and the ?resst data properties populated with the values indicated. In addition, the ?obl and ?clause instances are associated with the response as conditions to accessing the record.

V. CONCLUSION

Our prototype brings together the operational data in an EMR workflow for protecting genetic information privacy with the applicable laws, regulations and policies to provide a definitive and consolidated response for access and the associated pre/post conditions for use. Currently, we continue to implement additional Federal and State rules, policies and regulations to develop a comprehensive repository and rule base. The following phase in the prototype will build upon these capabilities for Federal/State laws and regulation enforcement to accommodate the policies and procedures for a selected medical organization. The resulting prototype will demonstrate the overall capabilities needed to meet the medical community's access requirements while balancing the individual rights to privacy and ownership of their genetic medical data.

REFERENCES

[1] M. D. Ritchie, E. R. Holzinger, R. Li, S. A. Pendergrass, D. Kim. "Methods of integrating data to uncover genotype-phenotype interactions." Nature Reviews Genetics 16.2. 2015. 85-97.

[2] A. H. Németh, A. C. Kwasniewska, S. Lise, R. P. Schnekenberg, E. B. Becker, K. D. Bera, ..., & K. Talbot. "Next generation sequencing for molecular diagnosis of neurological disorders using ataxias as a model." Brain 2013. awt236.

[3] C. Pihoker, L. K. Gilliam, S. Ellard, D. Dabelea, C. Davis, L. M. Dolan, ... & E. Mayer-Davis. "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." The Journal of Clinical Endocrinology & Metabolism 98.10. 2013. 4055-4062.

[4] W. W. Lowrance, & F. S. Collins. “Identifiability in genomic research.” SCIENCE 317. 2007. 600-602.

[5] A. L. McGuire, & R. A. Gibbs. "No longer de-identified." SCIENCE-NEW YORK THEN WASHINGTON- 312.5772. 2006. 370.

[6] F. D’Abramo, J. Schildmann, & J. Vollmann. "Research participants’ perceptions and views on consent for biobank research: a review of empirical data and ethical analysis." BMC medical ethics 16.1. 2015. 1.

[7] J. E. Lunshof, R. Chadwick, D. B. Vorhaus, & G. M. Church. "From genetic privacy to open consent." Nature Reviews Genetics 9.5. 2008. 406-411.

[8] The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Pub. L. 104-191, 110 Stat. 1936, codi_ed as amended at 42 U.S.C x300gg and 29 U.S.C x1181 et seq. and 42 U.S.C x1320d et seq.

[9] Genetic Information Non-discrimination Act of 2008 (GINA). Pub. L. 110-233, 122 Stat. 883, codified as amended in scattered sections of 26, 29, and 42 U.S.C.

[10] D. Mascalzoni, A. Hicks, P. Pramstaller, & M. Wjst. "Informed consent in the genomics era." PLoS Med 5.9. 2008. e192.

[11] L. O. Gostin, & J. G. Hodge Jr. "Genetic privacy and the law: an end to genetics exceptionalism." Jurimetrics 1999. 21-58.

[12] A. E. Prince and M. I. Roche. "Genetic information, non-discrimination, and privacy protections in genetic counseling practice."Journal of genetic counseling 23.6. 2014. 891-902.

[13] S. M. Liao. "Is there a duty to share genetic information?." Journal of medical ethics 35.5. 2009. 306-309.

[14] A. Lucassen, & J. Kaye. "Genetic testing without consent: the implications of the new Human Tissue Act 2004." Journal of medical ethics 32.12. 2006. 690-692.

[15] American Society of Human Genetics Social Issues Subcommittee on Familial Disclosure.

[16] ASHG STATEMENT Professional Disclosure of Familial Genetic Information. Am. J. Hum. Genet. 62 (1998): 474–483.

[17] E. Sherlock. “disclosure of patient's genetic information without their consent- Is the "public interset" really a Sufficient Justification?.” Genomics Law Report. 2009. retrieved March 2, 2015, from http://www.genomicslawreport.com/index.php/2009/11/10/disclosure-of-patientsgenetic-information-without-their-consent-is-the-public-interest-really-a-sufficient-justification/

[18] J. Kaye, S. M. Gibbons, C. Heeney, M. Parker & A. Smart. "Governing biobanks: Understanding the interplay between law and practice. " Bloomsbury Publishing, 2012

[19] D. Hallinan, & M. Friedewald. "Open consent, biobanking and data protection law: can open consent be ‘informed’under the forthcoming data protection regulation?." Life sciences, society and policy 11.1. 2015. 1.

[20] J. Kaye, C. Heeney, N. Hawkins, J. De Vries, & P. Boddington. "Data sharing in genomics—re-shaping scientific practice."Nature Reviews Genetics 10.5. 2009. 331-335.

[21] D. Mascalzoni, A. Hicks, P. Pramstaller, & M. Wjst. "Informed consent in the genomics era." PLoS Med 5.9. 2008. e192.

[22] J. Belmont, & A. L. McGuire. "The futility of genomic counseling: essential role of electronic health records." Genome medicine 1.5. 2009. 1.

[23] M. T. Scheuner, H. de Vries, B. Kim, R. C. Meili, S. H. Olmstead, and S. Teleki. "Are electronic health records ready for genomic medicine?." Genetics in Medicine 11.7. 2009. 510-517.

[24] M. H. Ullman-Cullere and J. P. Mathew. "Emerging landscape of genomics in the electronic health record for personalized medicine." Human mutation 32.5. 2011. 512-516.

[25] M. Gymrek, A. L. McGuire, D. Golan, E. Halperin, & Y. Erlich. "Identifying personal genomes by surname inference." Science 339.6117. 2013. 321-3