Appendix - Details of the selected studies

		Features									
Ref.	**Article Title**	**Confidentiality**	**Integrity**	**Availability**	**Privacy**	**Provenance**	**Authentication**	**Authorization**	**Category**	**Underlying mechanisms/technologies**	**Highlights**	**Similar to**
[38]	A fine-grained context-aware access control model for health care and life science linked data	-	-	-	-	-	x	x	Access Control	- XACML - OWL Ontology - SWRL rules - Inference/reasoning engine	- Publishers of Linked Data can define access conditions for their data by extending XACML with semantics - Access requests are evaluated by SWRL rules through a decision-making inference engine	[51]
[35]	A semantic authorization model for pervasive healthcare	-	-	-	-	-	-	x	Access Control	- Ontology - Inference/reasoning engine	- 4 layers authorization model - Ontologies encode context dynamics (concepts, relationships, policies, security rules) - Context-aware authorizations are granted through semantic reasoning	-
[51]	A SWRL bridge to XACML for clouds privacy compliant policies	-	-	-	x	-	x	x	Access Control	- XACML - OWL Ontology - SWRL rules	- Modelling of privacy requirements defined in data protection laws as privacy-aware access control policies - Semi-automated definition of XACML policies mapped from access control ontologies (good for existing and complex environments) - Access requests are evaluated by SWRL rules	[9], [38]
[57]	Access control management for e-Healthcare in cloud environment	-	-	-	-	-	x	x	Access Control	- XACML - OWL Ontology - SWRL Rules - RBAC security model	- RBAC security model supported by ontologies - A semantic knowledge base is queried for attributes of subjects and objects - XACML requests are created for access control evaluation	[35], [50]
[50]	An access control framework for pervasive mobile healthcare systems utilizing cloud services	-	-	-	-	-	-	x	Access Control	- OWL Ontology - SWRL Rules - Inference/reasoning engine - RBAC security model	- RBAC security model supported by ontologies - Captures the user's context through a mobile application - Provides automatic reasoning of access rigths to patient data and performs context-dependent temporary role changes for users	[35], [57]
[60]	Behavior-Based Access Control for Distributed Healthcare Environment	-	-	-	x	-	-	x	Access Control	- Ontology - Inference/reasoning engine	- Compares users' real and expected behavior and infer adequate access policies - Flexible solution based on semantic interoperability - Allows requests from different organizations without demanding changes in their systems' security architectures	[35], [50], [57]
[14]	Context-aware Access Control Using Semantic Policies	-	-	-	-	-	-	x	Access Control	- XACML - OWL Ontology - SWRL rules - Inference/reasoning engine	- Context-based access control policies are derivated from captured semantic contexts - The system suppresses user complexity of writing access control policies	[35], [38], [50], [57]
[36]	Establishment of access levels for health sensitive data exchange through semantic web	-	-	-	-	-	x	x	Access Control	- Ontology - Jena - JSON-LD - Semantic API	- Permissions are defined on ontology or property-level - Metadata-driven solution for system-level access control - Semantic responses are generated according to external systems' access level	-
[34]	Flexible access to patient data through e-Consent	-	-	-	x	x	-	x	Access Control	- Ontology - Abstract annotation model - RDF	- Provides a fine-grained access control mechanism based on electronic consent provided by the patient - Data is modeled and disclosed in RDF for semantic interoperability purposes - Solution based on abstract annotation model (less costly that standard annotation model)	-
[15]	Multi Authority Access Control in a Cloud EHR System with MA-ABE	x	-	-	x	-	x	x	Access Control	- Encryption (MA-ABE) - ABAC security model - Ontology - SWRL rules - Inference/reasoning engine	- Access policies are stored as SWRL rules - Users' attributes are extracted and confronted with policies - Provides flexibility for a complex environment where attributes differ among organizations.	[8]

Appendix - Details of the selected studies

		Features									
Ref.	**Article Title**	**Confidentiality**	**Integrity**	**Availability**	**Privacy**	**Provenance**	**Authentication**	**Authorization**	**Category**	**Underlying mechanisms/technologies**	**Highlights**	**Similar to**
[52]	Privacy compliance and enforcement on European healthgrids: An approach through ontology	-	-	-	x	-	-	x	Access Control	- OWL Ontology - SWRL rules	- Ontology-based approach for conflicting privacy and ethical requirements - Direct mapping of legislation to operational-level privacy-aware controls - Access control policies are defined as ontologies and SWRL rules are used for reasoning	-
[47]	Securing access to sensitive RDF data	-	-	-	x	x	-	x	Access Control	- Ontology - Abstract annotation model - RDF	- Presents a practical example of the solution presented in [34]	[34]
[39]	Semantic privacy-preserving framework for electronic health record linkage	-	-	-	x	-	-	x	Access control	- XACML - OWL Ontology - SWRL rules - Inference/reasoning engine	- Privacy preserving through a fine-grained access control mechanism - Promote secure electronic records linkage by controlling privacy risks based on semantic expressiveness	[38]
[17]	Towards a semantic medical internet of things	x	-	-	x	-	x	x	Access Control	- Ontology - RDF - IoT devices	- Semantic annotation and integration of healh data - Use of contract-based security policies	[2]
[5]	Using OWL and SWRL to represent and reason with situation-based access control policies	-	-	-	-	-	-	x	Access Control	- OWL Ontology - SWRL rules - Description Logic - Inference/reasoning engine	- Represents patient's data access scenario and perform inferences to either approve or deny access to data - Scenarios are modelled as ontologies and SWRL rules - The framework complies with the “need to know” principle for data disclosure	-
[8]	ARTEMIS: towards a secure interoperability infrastructure for healthcare information systems	x	x	-	x	-	x	x	Interoperability Infrastructure	- Semantic Web Services - Ontology - Inference/reasoning engine - Encryption (Triple-DES)	- Middleware for inter-organizational policies (architecture for functional, semantic and organizational interoperability) - Abstracts the differences in security requirements (roles, clinical concepts and policies) and capabilities of each system through reasoning	[15]
[59]	Secure semantic smart healthcare (S3HC)	x	x	x	x	-	x	x	Interoperability Infrastructure	- Ontology - SWRL rules - Inference/reasoning engine - SPARQL - RDF/XML Security - Encryption - Hash functions - IoT devices	- Collection, representation, storage, and integration of healthcare devices data - Implementation of several security layers/features - Doctors can securely analyze the collected data	[37]
[37]	Security Framework for Tuberculosis Health Data Interoperability Through the Semantic Web	x	x	x	-	-	x	x	Interoperability Infrastructure	- Ontology - Hybrid cryptography - Hash functions - Jena - SPARQL - D2Rq Server - HyperGraphQL - Semantic APIs - JSON-LD - RDF	- Integration with a semantic interoperability layer - Implementation of several security layers/features - Availability of several semantic endpoints (SPARQL, GraphQL, APIs)	[36], [59]
[9]	A Model-driven Privacy Compliance Decision Support for Medical Data Sharing in Europe	-	-	-	x	-	-	-	Privacy Compliance	- Ontology - SWRL rules - Inference/reasoning engine	- Ontologies are used to model the required domain and context information about data sharing and privacy requirements - SWRL rules allow reasoning about legal privacy requirements that are applicable to a specific context of data disclosure (considering different entities in European countries)	[51]

Appendix - Details of the selected studies

		Features									
Ref.	**Article Title**	**Confidentiality**	**Integrity**	**Availability**	**Privacy**	**Provenance**	**Authentication**	**Authorization**	**Category**	**Underlying mechanisms/technologies**	**Highlights**	**Similar to**
[2]	An integrated framework for privacy protection in IoT — Applied to smart healthcare	-	-	-	x	-	-	-	Privacy Compliance	- OWL Ontology - Inference/reasoning engine - IoT devices	- The framework integrates data collected from IoT medical devices - Inference engine to determine the privacy risks incurred when some personal data elements are shared with a data consumer. A list of risks and recommendations is provided to the data owner for informed decision-making.	[17]
[30]	An Ontology for a HIPAA compliant cloud services	-	-	-	x	-	-	-	Privacy Compliance	- OWL Ontology	- The ontology represents the HIPAA concepts (stakeholders, privacy and security rules) - Users can identify healthcare services that comply with the HIPAA act - Guidance for organizations to ensure HIPAA compliance	-
[16]	COC: An ontology for capturing semantics of circle of care	-	-	-	x	x	-	x	Privacy Compliance	- Ontology - RDF - SPARQL	- Captures the concepts and relations of the patient's circle of care - Compatible with HL7 FHIR standard - Data access logs are annotated with the COC ontology and converted into an RDF dataset that can be queried using SPARQL queries to investigate if a data consumer is in the circle of care of a patient and, therefore, can access the patient's data.	[10], [26], [46]
[10]	Improving privacy in health care with an ontology-based provenance management system	-	-	-	x	x	-	-	Privacy Compliance	- Ontology - SPARQL	- Patients define access permissions for their medical data - Domain ontologies support the detection of privacy violations by querying provenance data	[16], [26], [46]
[13]	Knowledge-based personalized search engine for the Web-based Human Musculoskeletal System Resources (HMSR) in biomechanics	x	-	-	-	-	-	-	Privacy Compliance	- OWL Ontology - Multi-agent semantic crawler for the Web - Asymmetric encryption	- A semantic crawler searches the web based on user-defined keywords - Results are encrypted using asymmetric encryption to protect medical information (confidentiality)	-
[46]	Ontology for Attack Detection: Semantic-Based Approach for Genomic Data Security	-	-	-	x	-	-	-	Privacy Compliance	- OWL Ontology - SWRL rules - SPARQL - Jena - Inference/reasoning engine	- Definition of an ontology to detect attacks on genomic data - The system analyzes incoming requests through a knowledge base of threat and inference rules - The ontology captures the context of attacks and threats for further analysis	[10], [16], [26]
[26]	Preserving patients' privacy in health scenarios through a multicontext-aware system	-	-	-	x	-	-	-	Privacy Compliance	- OWL Ontology - SWRL rules - SPARQL - Jena - Inference/reasoning engine	- Users can choose privacy policies to manage when, where, how, and to whom their private information can be revealed - Information about users and contexts is represented by ontologies and privacy policies are expressed as SWRL rules - A reasoner receives the ontological models and applies SPARQL queries	[10], [16], [46]