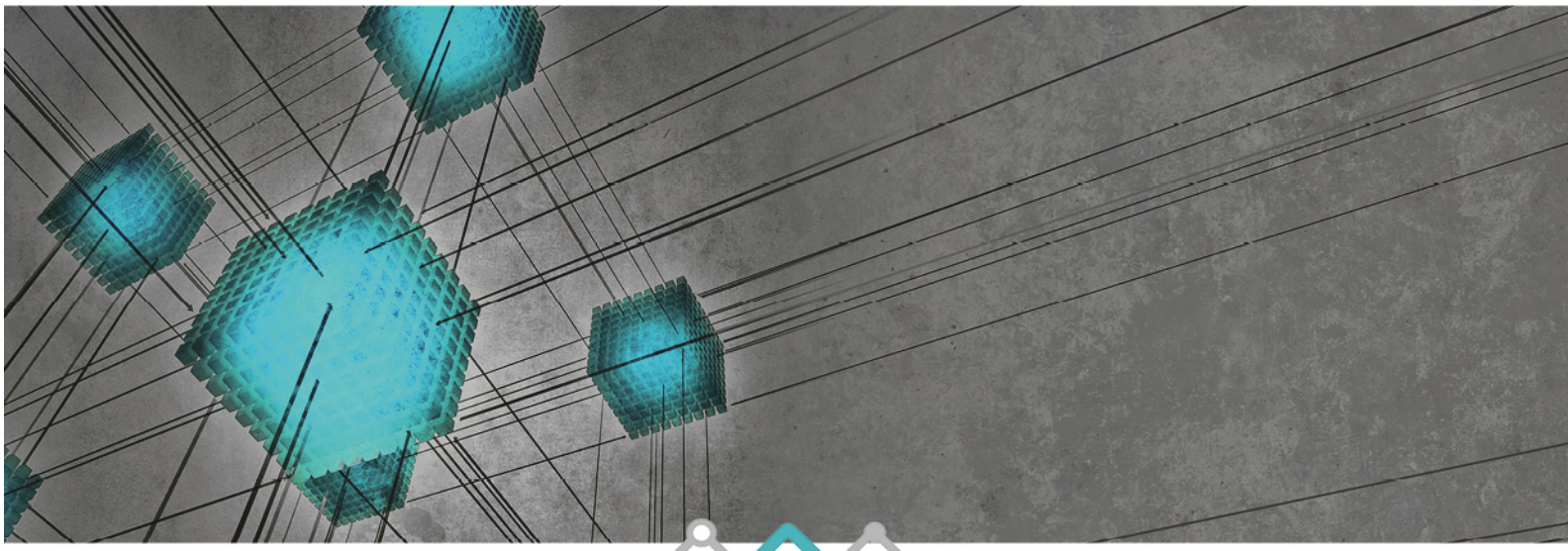

interiot

INTEROPERABILITY
OF HETEREOGENEUS
IOT PLATFORMS.

D8.4

Data Management Plan

June 2016

INTER-IoT

INTER-IoT aim is to design, implement and test a framework that will allow interoperability among different Internet of Things (IoT) platforms.
Most current existing IoT developments are based on ”closed-loop” concepts, focusing on a specific purpose and being isolated from the rest of the world. Integration between heterogeneous elements is usually done at device or network level, and is just limited to data gathering. Our belief is that a multi-layered approach integrating different IoT devices, networks, platforms, services and applications will allow a global continuum of data, infrastructures and services that can will enable different IoT scenarios. As well, reuse and integration of existing and future IoT systems will be facilitated, creating a de-facto global ecosystem of interoperable IoT platforms.
In the absence of global IoT standards, the INTER-IoT results will allow any company to design and develop new IoT devices or services, leveraging on the existing ecosystem, and bring get them to market quickly.
INTER-IoT has been financed by the Horizon 2020 initiative of the European Commission, contract 687283.

interiot

INTER-IoT

Data Management Plan

Pablo Giménez Salazar (VPF)
Eneko Olivares (UPVLC)
Anna Costa (ASL TO5)
Gianluca Aloi (UNICAL)
Miguel Llorente (PRODEVELOP)
Eric Carlson (RINICOM)
Marcin Paprzycki (SRIPAS)
Alessandro Bassi (ABC)

Edited by: Alessandro Bassi (ABC)

Reviewed by: Mariano Cecowski (XLAB)
Decebal Constantin Mocanu (TU/e)

Version: Final

Security: Confidential

June 30, 2016

The INTER-IoT project has been financed by the Horizon 2020 initiative of the European Commission, contract 687283

Disclaimer

Executive Summary

The Deliverable D8.4 aims to provide the guidelines and the rules for the management of the project's data and explaining how do we intend to make them available for third parties.

The project will collect data from different sources. For what regards m-health, in general all activities realized in this area are characterized by strong ethical behaviour. The operators' behaviour is aimed to respect personal dignity and privacy. As a consequence, the overall protection of the subjects' health data is a priority and will strictly follow the applicable laws on all matters related to Privacy. The procedures and forms related to the data handling are described in detail.

Concerning the logistic area, the most common and interesting actors for our scenarios are the port authority, the terminal and the hauliers that access to the port with goods. The port authority has multiple data streams to monitor the entire port area, and the sharing of that data will improve the efficiency of several processes. Furthermore, terminals manage big quantities of data coming from their machinery and workforce. The combination of this data with the operations and with external physical entities like trucks and containers opens new business opportunities. The last actor involved in the scenarios are road haulier companies. These companies have fleet management systems and sharing that data can significantly improve operational efficiency.

The INTER-IoT project plans to open a call for third parties to test the different components developed within the project. New applications will start producing data in the context of the platform development, validation and testing. This will make necessary a proper data management. The data coming from new (or at this point unexpected) domains will be initially classified by its level of sensitivity and handled in consequence.

Internally, several platforms are used to handle internal project data. In particular, HORDE, JIRA and some tools to manage the source code developed. These tools will be responsible for storing and managing internal information generated during the project. HORDE offers applications such as a groupware package with a calendar, notes, tasks, file manager and a Wiki. The Atlassian JIRA tool is used for data collection and tracking, including software issues and requirements. Finally, documents that require a collaborative approach will be held on Google Docs privately, since a real time edition tool is not available for the Horde platform.

The Inter-IoT project is fully committed to opening all possible deliverables and data sets to the public, fully respecting the existing regulations and the specific provisions of the Consortium Agreement. It should be noted that access to some datasets generated during the INTER-IoT project will be guided by legal requirements imposed by parties outside of the INTER-IoT consortium. This concerns primarily, scientific publications. In each such case, a link to the publication will be provided within the INTER-IoT web portal.

Contents

List of Figures

Acronyms

PC	Project Coordinator
D#.#	Deliverable number #.# (D2.1 deliverable 1 of work package 2)
DoA	Description of Action of the project
INTER-IoT	Interoperability of Heterogeneous IoT Platforms
EC	European Commission
EU	European Union
GA	Grant Agreement
H2020	Horizon 2020 Programme for Research and Innovation
IoT	Internet of Things
IPR	Intellectual Property Rights
M#	#th month of the project (M1=January 2016)
WP	Work Package
IPR	Intellectual Property Rights
PCC	Project Coordination Committee
PIC	Project Implementation Committee
STPM	Scientific and Technical Project Manager
TL	Task Leader
WPL	Workpackage Leader

1 Introduction

The Deliverable D8.4 aims at providing the guidelines and the rules for the management of project's data and explaining how do we intend to make them available for third parties.
Section 4 of Deliverable D8.3 provided a brief overview of the data management policy that will be used as guideline for all project partners with regard to the datasets that will be generated by the project. As the INTER-IoT project will collect sensitive data from various sources, precise guidelines must be established in order to protect non-authorised access to sensitive data and, at the same time, guaranteeing the widest possible dissemination of the project results through the use of Open Access policies as stated in the H2020 plan, namely in the document "Open Access to Scientific Publications and Research Data in Horizon 2020".
This deliverable is divided in 3 main sections: Section 2 will be analysing how the project will collect data, Section 3 will be about how the information is stored within the project, and the Section 4 will show how the project will try to widen as much as possible the dissemination of results and the availability of data.

2 Data harvested by the project

2.1 m-health data

The ASL TO5 aims are the protection of the mental and physical health and the improvement of the people life quality.
All health activities performed to achieve these objectives are characterized by ethical behavior.
For this reason the operators behavior is aimed to respect the personal dignity and privacy that every ASLTO5 citizen has right, and is adapted to the various situations in which the benefits were provided.
Consequently the overall protection of the subjects health data is a priority of our company that has applied in full and concrete Italian law on all matters related to Privacy.
Therefore, our organization is therefore concerned to manage properly, for the protection of individuals and communities, the collection, recording, organization, storage, consulting, development, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, deletion and destruction of data; in a word, the "treatment" of the data, defining general procedures and special instructions for the staff.
The criteria and methods used are also applied to activities carried out for the project INTER-IoT.
The subjects assigned to data processing are:

- Data Controller, ASL
- Data Processor, Corporate Structures Directors
- Person tasked with processing, Employees and Collaborators
- External Data Processor, Companies outside the ASL

2.1.1 Data Processor Appointment Letter (”Atto di Nomina del Responsabile al trattamento dei dati”)

With Institutional Determinations the ASL as ”Data Controller” appointed the ”Data Processors” in the persons of the Corporate Structures Directors. Directors should ensure respect and compliance with the Code of Privacy [1] and its security measures [2] within its structure; following the instructions of the Data Controller they must ensure appropriate measures to guarantee dutiful behavior of rights, freedoms and dignity of patients.
The Company, in order to manage properly the security and privacy of personal and health data, explaining to the operators approach to be taken in the various cases ranging from the direct relationship with the patient, to the imputation of the data on your computer, protection during the maintenance of

[1] Legislative Decree 30 June 2003, n.196 ”Codex on protection of personal data”
[2] Legislative Decree 30 June 2003, n.196 ”Codex on protection of personal data”

the equipment, etc, it also has instructions and procedures aimed at all employees (Security Policy Document of 2011). Fundamental task of the Corporate Structure Director is to observe and enforce the precautions identified in this document.

2.1.2 Data Processing Figure Appointment Letter and Data Processing Temporary Figure Appointment Letter (”Atto di Nomina dell’Incaricato al trattamento dei dati” and ”Atto di Nomina dell’incaricato temporaneo al trattamento dei dati”

Employees and Collaborators appointed "Person Tasked with Processing" (employee) or "Temporary Person Tasked with Processing" (not employees) by the Company Structure Director (Data processor) are people authorized to perform processing operations such as collection, recording , storage, consultation, modification, selection, extraction, use, communication, dissemination, erasure and destruction of data, even if not registered in a database. It is countersigned and filed forms from the organization that determines an individual responsibility of the individual employee or collaborator that is proportionate to their role but also functional to an adequate processing of data in the various practical situations in which the operators are in contact with citizens. The specific Instructions can be found in Annex.

2.1.3 Data Processing Instructions (”Istruzioni per incaricati al trattamento dati”)

The responsibilities of employees and collaborators are not generic but selected from a list of specific instructions that each operator takes countersigning the indicated form. It is requested each "Person Tasked with Processing" to follow specific instructions for the processing of data, for the use of tools for the treatment and the respect of "Minimum Security Measures." The commitments made in the processing of personal and health data impose appropriate behaviors that concerns a direct relationship with the patient, instruments and equipment or computer equipment.
The specific Instructions can be found in Annex.

2.1.4 External Data Processor Appointment Letter (”Atto di Nomina Responsabile Esterno”)

Since the ASL TO5, is the Data Controller of the data mentioned above, the Company Structure Director as Data Processor may appoint as "External Data Processor" all external parties who carry out processing operations of personal or sensitive data. During the course of the project INTER-IoT protection of data collected directly through mobile devices and data stored on external platforms not controlled and managed by the ASL TO5, are the responsibility of the respective Partners participating in the project as a ”External Data Processor”.

2.2 Transport and logistics data

One of the two application domains of the INTER-IoT project is transport and logistics around ports. In this environment there are many actors involved in port activities, so all data must be taken into account.

2.2.1 Data owners

The most common and interesting actors for our scenarios are the port authority, the terminal and the hauliers that access to the port with goods.

One of the key players is the port authority, as it manages a wide variety of data. The port authority has multiple sensors to monitor the entire port area. It has data recorded from all companies that interact with the port and data from other integrated systems in the port such as the automatic gates. The main motivation of the port authority to share some of this data is to improve the efficiency of some processes such as the access of vehicles to the port and to reinforce security, safety and environmental friendly aspects. The acquisition of sensor and other data coming from physical entities and its management and storage in an interoperable IoT platform open new opportunities to combine it with other sources of data inside the organisation and along the port infrastructure. Other important actors are the container terminals in the port. Terminals manage big quantities of data coming from their machinery and workforce. The combination of this data with the operations and with external physical entities like trucks and containers open new business opportunities. Knowing the exact times of arrival of trucks, for delivery or collection of containers allows a better planning, optimise operations and save considerable time.
The last actor involved in the scenarios is road haulier companies. These companies have fleet management systems that manage all data from their trucks but the data generated by these physical entities are not shared along its route with the different infrastructures. The trucks usually have to wait at the entrance of the port or for its container to be ready. Share information with the port and the terminal can significantly reduce these times.

2.2.2 Data sources

This section details the data and their sources that will be gathered in the INTER-LogP pilot, produced by the main actors previously mentioned.

2.2.2.1 Port

The port environment produces several data from different sources. On the first hand, data is collected from the port industrial network and the SCADA (Supervisory Control And Data Acquisition) system. This system is used for remote monitoring and control in the Port Authority facilities. It has weather station measurements such as temperature, wind, air quality, water quality, and wave and tidal data from the buoys and many other kinds of sensors data. Some additional information that could be obtained from the industrial network of the port is traffic management (including the automated gate system), security and safety related data, as well as data coming from the automated identification system (AIS) for vessels.
On the other hand, data from the Port Community System (PCS) will be sourced at application level and combined with data coming from physical entities. ValenciaportPCS is a technological platform created by the Port Authority of Valencia providing services designed to streamline and facilitate the operating processes of companies of the port community through electronic documentation and data sharing among the companies conforming the port community. The Valenciaport PCS offers a single source of information on departures and arrivals of vessels, dangerous goods, loading and discharge lists, road transport delivery and gate in/gate out orders, shipping instructions, customs information, etc.

2.2.2.2 Terminal

From the Port Container Terminal, it is expected to receive for instance data from the machinery that handles and moves containers inside the terminal. This data is obtained from PLCs (Programmable

Logic Controllers) located inside every machine working at the terminal, collecting about 80 signals per second per machine.
These signals or data are related to location (GPS coordinates), quality of the signal, orientation, type of machine, gantry status, bloom status and alarms due to failure and container position.
As well the Port Container Terminal would be expected to send data from their Terminal Operating System (TOS) such as the work orders to move the container, including information about the container plate, the location inside the container yard or in the vessel and several other operational parameters.
Many other signals could be received from the SEAMS platform. The Smart Energy efficient Adaptive Management System (SEAMS) platform is a monitoring tool that is able to monitor the different operations being carried by the equipment and machinery used at Noatum Container Terminal Valencia (NCTV) thanks to a complete mobile sensor network that has been created. This information includes the location of the different cranes, speed, working hours, fuel levels, position of the spreader and lighting information to make the use of energy more efficient.

2.2.2.3 Road Haulier companies

Road haulier companies are expected to collaborate in the INTER-LogP pilot. These companies are responsible for the movement of containers by road and therefore their trucks must access the port and the terminal. They have a fleet of trucks of different sizes and they may even subcontract other trucks to carry out their jobs. To manage all their assets they use fleet management systems. This system manages the transport operations of the company and receives data from sensors and devices installed in the truck (data coming from the CAN bus, GPS, tachograph, anti-theft, etc.). The most relevant data for road haulier companies is the location of the trucks but there are many other information that is useful like the driving hours registered at the tachograph fitted in the vehicle, the fuel level, temperature of the reefer container or trailer, container being transported and some other information regarding security and anti-theft systems like tamper proof RFID and active e-seals that are installed on the trailers and containers. Finally, the interactions of the truck with the infrastructures can provide several benefits in terms of optimisation, safety and security.

2.2.3 Data Management

The data captured, handled and provided by these organisations for the research of INTER-IoT will be used under a confidential and non-disclosure agreement. In the case personal data is obtained (i.e. driver's details), the acquisition of these data will need to obtain the authorisation of the person concerned and respect personal protection laws.
On a first stage the research team will analyse, characterise and select the data that will be associated with the different scenarios to be demonstrated and the data available from different sensors, devices, networks and platforms considered in these scenarios. During the first experimentations, simulated data or experimental data could be generated and used for simplicity and in order to test specific conditions in a lab environment that are difficult to obtain in a real environment. Once these first experimentations are correctly done, the products developed will also be tested under real conditions during the pilots.
The data captured during the experimentations and pilots, will allow the generation of different metadata models and ontologies adapted to the general use of INTER-IoT along different domains but able to be also adjusted to the specificities of the port, transport and logistics needs.
Data sets captured during the research will be anonymised in terms of times (i.e. date when the information was captured), physical entities identification (i.e. vehicle plates, container numbers), organ-

isations and personal data, so they will be able to be used in future researches and demonstrations without compromising any sensitive or commercial concerns from the actors involved. Anonymization will be considered in the design of the data models and using transformation algorithms.

2.3 Other Data

INTER-IoT aims to be a helpful platform or framework allowing inter-operation between very different application domains. So that, although the very initial design will consider the archetypes of health and logistic domains, it will soon be expanded across other fields. With this in mind, the data management also needs to be though from a global point of view.
Specifically, within the INTER-IoT project it is planned to open a call for third parties to test the platform developed and integrate with it. In that point of the project, new applications will start producing data in the context of the platform development, validation and testing. This will make necessary a proper data management as done in the INTER-IoT initial devised pilots. However, the inability to know at this moment the application domain or even the field of the pilot(s) that could be integrated as a consequence of the open call, reveals the need of defining a plan for generic data collection and management.
The data coming from new (or at this point unexpected) domains will be initially classified by its level of sensitivity following the following table:

Data Class	Adverse Business Impact	Sample data (not exhaustive list)
Protection level 3	Extreme	Data that creates extensive ”shared-fate” risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles.

Protection level 2	High	Data elements with a statutory requirement for notification to affected parties in case of a confidentiality breach: • Social security number • Driver's license number, ID number • Financial account numbers, credit or debit card numbers and financial account security codes, access codes, or passwords • Personal medical information • Personal health insurance information
Protection level 1	Moderate	Information intended for release only on a need-to-know basis, including personal information not otherwise classified as Level 0, 2 or 3, and data protected or restricted by contract, grant, or other agreement terms and conditions, e.g.: Business: • Number or kind of sensors used in private environments • Business sensitive data • Licensed software/software license keys • User subscriptions to electronic resources

Protection level 0	Low	Information intended for public access, e.g.,: • Public directory information • Public websites • Open data

Table 2.1: Other Data

The gathered data in INTER-IoT will be labeled with one of the protection levels in its meta-data, allowing to access to the protection level in any layer of INTER-IoT anytime. This level will not be able to be modified anywhere within or out the platform, so the classification must be defined according the guidelines by the data-producer (the integrator).
Additionally, data treatment guidelines and rules will be applied to the new data sources, with special attention to personal and business sensitive data. In the case that newly connected platforms produce personal data or information, then a general policy of anonymization will be applied. This will consist in the assignation of a numeric or alphanumeric ID to the user, which will represent it from then and on in the INTER-IoT platform. The correspondence between personal data and the INTER-IoT ID will be stored in a separate database only accessible by the integrator. Personal data will not be stored in INTER-IoT and this will not be accessible without a direct contact with the data producer company, which will hold always the responsibility of disclosing that information within their own privacy, protection and security policies.
Business sensitive data such as IDs, credential or passwords will not be stored or communicated through INTER-IoT platform. The data producer or integrator will be responsible to share this when appropriate using their own channels to ensure the security of the information.
Preliminary data from integrators such as data formats, sample data-sets or business descriptions will be collected by forms, interviews or specific requests to be defined. This data will be protected, with the only access to the Consortium members in charge to ensure a correct integration or to facilitate this. This data will be stored physically or electronically using the project's storing resource and applying password and/or encryption when necessary or specifically requested by the party.

3 Data within the project

3.1 Internal Data Handling

Several platforms have been used to handle internal project data. In this section, the following tools are presented: HORDE, JIRA and some tools to manage the source code developed. These tools will be responsible for storing and managing internal information generated during the project. HORDE offers applications such as a groupware package with a calendar, notes, tasks, file manager and a Wiki. Data collected or generated relevant for the project is stored in the Horde platform deployed for the project. The Atlassian JIRA tool is used for data collection and tracking, including software issues and requirements. Each partner has a username and password to access these platforms with all content editing permissions granted. If an external person needs to access to some data, he or she will be granted access only to the requested information in case this inquiry is accepted. Also, to ensure that the data can be easily recovered, it will be explained in this section how to perform backups of the internal data. This is a key feature of the plan as we will work with several datasets accessed by different partners with different technical skills. Documents that have to be edited too often, or that need a more collaborative approach (such as action points and tracking spreadsheets, audioconference minutes, draft agendas, etc.) will be held on Google Docs privately, since a real time edition tool is not available for the Horde platform.

3.2 Horde

The project will setup a private collaborative workspace based on Horde. It is an open-source groupware software including many features, though the File Manager will be the most relevant one. Respective accounts for each partner are managed by the system administrator and new accounts can be created as needed, including re-arrangement of existing users. Horde is used for internal access and document management. This restricted groupware working space includes the following sections:

- Contractual documents – Grant Agreement, Consortium Agreement, etc.
- Resources – actual information on usage of the resources.
- Deliverables – completed, submitted, reviewed
- WP and Task workspaces – to share and work collaboratively on respective documents, draft deliverables, concept papers, etc.
- Dissemination – to store and work together on dissemination items; e.g. papers, call for papers or workshops organisations

- Templates – to include deliverable and presentation templates, project and partnersÕ logos, etc.
- Meetings – with agendas and minutes from physical meetings, notes from audio conferences, action points agreed, etc.
- Coordination with standardization organizations
- Coordination with ICT30-EPP projects through the IoT-EPI group and the six Task Forces organised to carry out the different activities.

The working space structure will be extended as needed by the project consortium and individual partners for their work in the project as well as to serve as file sharing platform among the consortium members. UPV research team will act as administering body of the server, however any partner can request resources on demand.

3.3 Jira

Jira is an issue tracking tool, but in the project will be also used to store and track collaborative data based on templates (e.g. requirements, scenarios or risks have been defined). This tool will host only internal data and is only accessible with an account, protected with user and password. Jira will be used to collect the following data:

- Market Analysis – Existing products and stakeholders identified by each partner.
- Project Management – Potential risk gathering and tracking.
- Project Development – Definition and tracking of scenarios, use cases and requirements.

During the project lifetime can be defined new template-based datasets to be collected and stored in Jira, as well as issue tracking of the developed software.

3.4 Source Code Versioning

During the project we will proceed to handle the source code of the applications using a version control system (VCS) tool, in order to nimbly manage the changes of the code and to reverse them in case something unexpected happens. Within this version control system, we will define different levels of credentials for users, such that several users could access to most of the code and one or few administrator can configure and control the whole system.

3.5 Data Back-up

INTER-IoT data support services (HORDE platform, JIRA and VCS) are hosted by UPVLC on a Linux server. The disks of these servers are mirrored to protect against initial hardware failures. In addition, the following backup procedures are implemented:

- Full system backup of the server is made on a weekly basis and stored on a separate backup server. The full system backups are on a per-file basis and are uncompressed to ensure fast turnaround times for restore jobs. Latest weekly backup is also copied offsite.

- A 30 days backlog of full system backups is kept.
- A daily backup of all the content in the Horde platform and JIRA tool is performed and stored on a separate backup server.
- Since content backups are run on a 24 hours interval, a file saved on the Horde platform is only guaranteed in the backup after maximum of one day.
- SQL Databases are dumped to plain serialized files before backup to ensure there is no corruption. If some of the services are used from external providers, which might be necessary and therefore decided by the consortium, copies of all public repositories are stored on the Horde server which is hosted by UPVLC and to which the aforementioned backup procedures apply.

3.6 External data distribution

External data will be distributed following the guidelines specified in D1.2, according to the Horizon2020 procedures and the Open Research Data Pilot recommendations. In summary, the following datasets will be distributed through these channels:

- Research publications – Will be accessible from the project website and the two data repositories mentioned in D1.2 (after the period of embargo has ended for green type open access publications or immediately for the gold type).
- Software source code – Will be released as open access once a stable version is produced. It will be accessible from the webpage and from public source code repositories.
- Software binaries and documentation – Along with the source code, compiled versions with guides and documentation will be accessible from the project webpage.
- Other research data – Other data collected from analysis and evaluation will be accessible as well from the project webpage and will also be published to the same open repositories used for research publications, e.g. (white papers and tutorials/key note presentations).

4 Data generated by the project

4.1 Project deliverables

As in all projects that involve commercial and academic partners, deliverables (data sets generated during the project) can be divided into two general categories:

(i) public, and

(ii) internal to the consortium.

The Inter-IoT project is fully committed to opening all possible deliverables (data sets) to the public. However, recall that the two use cases involve commercial partners. Therefore, some information concerning, for instance, details of the implementation of platform interoperability within the two sites may need to remain private to the project partners. All necessary details, concerning which deliverables may remain private and how they are going to be handled, are contained in the Consortium Agreement.

This being the case, standard procedure applied in such situation, in EU-funded projects, will be applied. All deliverables will be placed in, and made available from, the Inter-IoT dataset repository. Here, the public datasets will be made available through the Inter-IoT web portal. At the same time, access to the private datasets will require logging in to the repository (via username and password). Login information will be provided to the project partners as well as authorized EU officials.

It should be noted that access to some datasets generated during the Inter-IoT project will be guided by legal requirements imposed by parties outside of the Inter-IoT consortium. This concerns, primarily, scientific publications. As stated in Section 4.2, while striving for open access to scientific publications, some of them will have to be published in closed access journals / books. In each such case, a link to the publication will be provided within the Inter-IoT web portal.

The publication itself will then be available only after satisfying requirements of the publisher (these requirements, as well as exceptions to them, vary from publisher to publisher , and thus cannot be specified further). In the case of open access publications we will still provide a link to the publication, but in this case it will be fully available to anyone. However, storing copies of all publications within the UpV server will be considered. In case this decision will be made, publications will be stored in the private part of the repository (to avoid any copyright conflicts).

Information about publicly available datasets will be disseminated according to the strategy formulated in D8.3. This document contains detailed strategy concerning whom and through which channel will have results delivered. This document should be consulted for further details.

All deliverables will be stored within the computer infrastructure provided by the UPV.

4.2 Scientific Publications

According to the dissemination strategy, planned in D8.3 (Impact Creation Plan), theoretical and experimental results of INTER-IoT will be disseminated trough major international technical journals, magazines and peer-reviewed conferences.
All these scientific publications will be accessible to external sources on a specific section of the INTER-IoT website. This section will include also publications finalized after the project is completed.
According to the open access policy of INTER-IoT project, a golden model will be preferred to reach maximum impact. Thus, publications under open access rules will be hosted in the INTER-IoT website, where the publication download will be directly available together with the web link to the original contribution hosted by the open-access publishing company.
On the other hand, a high number of publications, that will target a very high impact (i.e. most read and cited), are constrained by closed or partially closed copyright policies. Frequently, a publication under copyright rules is preferred to reach a high impact that, often, is facilitated by the high reputation of several publishing company in the scientific community. In such cases, if applicable, we will refer to a green model. Indeed, some important publishing companies (e.g. IEEE, Elsevier, ACM) allow authors to post their own version (i.e. ”preprint” or ”accepted” version) of their articles, on their personal author’s home page, or on the owner’s institutional repository, or in any repository legally mandated by an agency funding the research on which the Work is based, or in any non-commercial repository. In such cases, scientific publications will be hosted directly in the INTER-IoT website or a web link to the allowed repository (i.e. by copyright rules) will be provided.
In few cases, copyright policies (e.g. Springer, Wiley) apply an embargo period of 12-24 months prior to allow a green like model. In such cases, scientific publications will be available in the INTER-IoT website only after the embargo period. In the meanwhile, only an abstract of the scientific publication will be provided.

4.3 Other publications and outputs

The consortium will continually identify interesting and relevant channels to promote the project and its results. As a supplement to project deliverables, scientific publications and contributions to industry standards, additional resource will be spent to engage non-consortium members. As with all project activities, generation of additional outputs from Inter-IoT will be undertaken in accordance with the grant agreement, consortium agreement and Commission legal requirements and policies regarding data protection, ownership, exploitation rights and confidentiality. Inter-IoT will use its project social media accounts and website to facilitate the circulation of project outputs and press releases in an attempt to engage with a wide range of the public. Consortium members will also utilize their own social media accounts and websites to gain publicity directly with their professional networks. Interviews and traditional media will be utilized to raise project profile when access is available. Material from the project will also be presented at conferences, in educational environments and workshops. Organization of public workshops will allow discussion with experts from the European research community. The advisory board will promote the Inter-IoT to industrial stakeholders which could benefit from inclusion in the workshops. World-wide dissemination tours and industry organized seminars will be utilized to engage with stakeholders. Large project achievements will be highlighted to raise the profile of Inter-IoT and inspire by-in and early adoption of the products produced in the project. A dissemination package including videos, blogs, press releases and newsletters will be produced each year to explain Inter-IoT’s impact on everyday life.

Output	Description
Websites	The project website and individual partner websites will be utilized to promote project work and promote other project outputs. This will target business networks connect to consortium members and the general public. This will be maintained from M1 to the end of the project.
Educational Environments and Conferences	World-wide dissemination tours and industry-organized seminars at universities will take place annually. Presentation of project outputs in conferences will be more frequent (total of 5 over the project's lifetime.
Interviews	Traditional media will be utilized when available.
Social Media	Social media presence will be maintained throughout the life of the project to promote results and opportunities for engagement with Inter-IoT.
Workshop materials	IoT results will be presented near the end of the project to demonstrate to the scientific and industrial communities. A total of 2 over the project's lifetime will be conducted.

Table 4.1: Other Communications

4.4 Contribution to standards

As there are no clear boundaries to the IoT domain, quite a number of standardisations are relevant for this sector. INTER-IoT will interact with several standardisation bodies at different levels in order to be part of the definition of standards for the whole IoT sector. Some of the standardization bodies that will be examined are:

- ETSI through the M2M standardization initiatives, including oneM2M;
- IETF through different efforts like ROLL, CoRE, 6LoWPAN;
- IEEE through the IEEE-SA and Standard IEEE P2413 propose an Architectural Framework for the Internet of Things (IoT)
- ITU-T, with particular regards to SG13 activities.

The project will also monitor Industrial initiatives like AllSeen Alliance, Open Interconnect Consortium, Thread Group or Industrial Internet Consortium as they target different aspects related with interoperability that will be addressed by the consortium, specifically in the INTER-FW and INTER-Layer outputs.
INTER-IoT is aware that worldwide-harmonised standardisation will be one of the key factors of the success of IoT concepts. Our strategy concerning standards consists of different actions:

- We will build our framework on open solutions to a maximum feasible degree. In the same spirit, we will also strive for a maximum compliance with existing open standards;
- We will associate standard organisations to the project by working with them since we will have noticeable results;
- By so doing we will create an early awareness for our efforts and achievements, and we will also prepare the ground for new standardisation activities, so as to encompass outreaches to pertinent standardisation groups at associated and other standard associations.

A Instructions for Data Treatment

Allegato 1)

NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI

L'Azienda Sanitaria Locale 8, nella persona del suo legale rappresentante in qualità di Titolare del trattamento dei dati personali da essa operato, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali"e in applicazione delle determinazioni n. 655 del 26.4.07 e n. _____ del _____ , dato atto che a tutti i responsabili è stata data la possibilità di partecipare ad apposito corso di formazione

DESIGNA

Il Dott. / La Dott.ssa _____
nella Sua qualità di Dirigente Responsabile della Struttura Complessa _____

RESPONSABILE DEL TRATTAMENTO DEI DATI TRATTATI DALLA STRUTTURA COMPLESSA _____

ai sensi dell'art. 29 del citato Codice in relazione al trattamento dei dati personali effettuato nella Struttura medesima.
Il Dott. / La Dott.ssa _____ in qualità di Responsabile del Trattamento dei dati nell'ambito della Struttura Complessa _____ , ha il potere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni in materia.
In particolare dovrà:

- osservare e fare osservare le precauzioni individuate nel documento programmatico sulla sicurezza dei dati personali e nelle circolari attinenti alla materia approvate dall'azienda;
- predisporre misure adeguate al rispetto dei diritti degli interessati, tenuto conto di quanto disposto dagli articoli del Codice 7 - diritti dell'interessato, 13 - informativa e 83, (ordine di chiamata prescindendo dall'individuazione nominativa, istituzione di distanze di cortesia, prevenzione dell'indebita conoscenza da parte di terzi di informazioni sullo stato di salute, impedimento di situazioni di promiscuità nelle prestazioni sanitarie, adozione di modalità adeguate per l'informazione ai terzi legittimati in occasione di visite agli interessati) il cui contenuto viene integralmente richiamato;
- verificare e confermare la presa in carico dei trattamenti attribuiti in via sperimentale alla propria struttura come da allegato;
- per ogni trattamento compilare e/o aggiornare **entro il 15 marzo** di ogni anno le **schede anagrafiche di trattamento** secondo lo schema e con le modalità che saranno comunicate successivamente all'avvio della procedura informatizzata per la gestione dell'anagrafe trattamenti;
- comunicare alla s.c. sistema informativo l'inizio di ogni nuovo trattamento nonché la cessazione o la modifica dei trattamenti già in essere;
- entro un anno dalla presente nomina, individuare e nominare per iscritto gli incaricati al trattamento e predisporre norme scritte per gli incaricati medesimi;
- interagire con il Titolare in caso di richieste di informazioni o effettuazione di controlli e accertamenti da parte dell'Autorità Garante per la protezione dei dati personali;
- informare prontamente il Titolare di ogni questione rilevante ai fini della legge;

Al presente atto di nomina viene allegato l'elenco dei trattamenti attribuiti in via sperimentale.
Al Responsabile del trattamento vengono inoltre forniti i seguenti documenti, scaricabili dal sito aziendale area interna:

- ***decreto legislativo n. 196/2003;***
- ***regolamento regionale per il trattamento dei dati sensibili e giudiziari delle Aziende Sanitarie, approvato con D.P.G.R. 11.5.2006 n. 3/R;***
- ***documento programmatico per la sicurezza anno 2006;***
- ***determinazione n. 655 del 26.4.2007 "Approvazione documento programmatico per la sicurezza e altre disposizioni in materia di privacy"***
- ***determinazione n. del "Approvazione schema atto di nomina dei responsabili del trattamento dati e scheda anagrafica di trattamento (versione sperimentale)";***

IL TITOLARE
Legale Rappresentante dell'A.S.L. 8
Dott. Giovanni Caruso

A.S.L. TO5
Azienda Sanitaria Locale
di Chieri, Carmagnola, Moncalieri e Nichelino

Sede Legale –Piazza Silvio Pellico 1 – 10023 Chieri (To) – tel. 011 94291 – C.F. e P.I. 06827170017

ATTO DI NOMINA DELL'INCARICATO AL TRATTAMENTO DATI

Il sottoscritto _____ in qualità di Direttore della S.C_____ nonché Responsabile del trattamento dati a seguito della nomina conferita dal Titolare, con il presente atto, in applicazione dell'art. 30, D.Lgs 196/2003,

nomina

il/la signor/a _____
dipendente dell'ASL TO 5, con la qualifica di _____
Incaricato/a al trattamento dei dati personali, sensibili, genetici, giudiziari la cui conoscenza ed il cui trattamento siano strettamente necessari per adempiere ai compiti assegnati, in relazione alle attività svolte nell'ambito del proprio settore di competenza e di quant'altro definito di volta in volta dal Responsabile.

Nel presente atto di nomina si fissano le **regole generali** a cui l'Incaricato/a deve attenersi nello svolgere le operazioni di trattamento dati che gli competono. Le specifiche operazioni di trattamento rientrano nelle istruzioni correlate a ciascuna procedura, procedimento, affare o pratica.

Pertanto l'Incaricato/a del trattamento dei dati, nel rispetto di quanto stabilito dal D.Lgs. 196/2003, dovrà:

- trattare i dati in modo lecito e secondo correttezza;
- raccogliere e registrare i dati per scopi inerenti l'attività svolta;
- verificare, ove possibile , che siano esatti e, se necessario aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono raccolti e successivamente trattati, secondo le indicazioni ricevute dal Titolare o Responsabile;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Responsabile;
- mantenere la massima riservatezza sui dati predetti;
- adottare le misure e gli interventi per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati, disposti dal Titolare o dal Responsabile;
- osservare le misure di sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito dei dati personali e in particolare osservare le istruzioni contenute **nell'allegato A)**;
- osservare scrupolosamente le disposizioni organizzative e operative impartite dal Titolare o dal Responsabile per il corretto, lecito, pertinente e sicuro trattamento dei dati custodire e controllare i dati personali oggetto di trattamento in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta;
- accedere ai soli dati personali la cui conoscenza sia strettamente necessaria in relazione e per l'adempimento delle mansioni e dei compiti assegnati;
- accedere, per esigenze di servizio, esclusivamente alle banche dati informatiche del proprio Servizio/Ufficio a cui è stato autorizzato dal Titolare o dal Responsabile;
- segnalare al Titolare o al Responsabile eventuale problemi applicativi rispetto all'attuazione e all'adempimento degli obblighi previsti dal D.Lgs. 196/2003.

Luogo e data _____
Firma del Responsabile del trattamento dati_____
Firma dell'Incaricato/a al trattamento dati_____

A.S.L. TO5
Azienda Sanitaria Locale
di Chieri, Carmagnola, Moncalieri e Nichelino

Sede Legale – Piazza Silvio Pellico 1 – 10023 Chieri /To) – tel. 011 94291 – C.F. e P.I. 06827170017

ATTO DI NOMINA DELL'INCARICATO TEMPORANEO AL TRATTAMENTO DATI

Il sottoscritto _____ in qualità di Direttore della _____ nonché Responsabile del trattamento dati a seguito della nomina conferita dal Titolare, con il presente atto, in applicazione dell'art. 30, D.Lgs 196/2003,

nomina

il/la signor/a _____ in qualità di _____

Incaricato/a temporaneo/a al trattamento dei dati personali, sensibili, genetici, giudiziari la cui conoscenza ed il cui trattamento siano strettamente necessari per adempiere ai compiti assegnati, in relazione alle attività svolte nell'ambito del proprio settore di competenza e di quant'altro definito di volta in volta dal Responsabile.

Nel presente atto di nomina si fissano le **regole generali** a cui l'Incaricato/a temporaneo/a deve attenersi nello svolgere le operazioni di trattamento dati che gli competono. Le specifiche operazioni di trattamento rientrano nelle istruzioni correlate a ciascuna procedura, procedimento, affare o pratica.

Pertanto l'Incaricato/a temporaneo/a del trattamento dei dati, nel rispetto di quanto stabilito dal D.Lgs. 196/2003, dovrà:

- trattare i dati in modo lecito e secondo correttezza;
- raccogliere e registrare i dati per scopi inerenti l'attività svolta;
- verificare, ove possibile , che siano esatti e, se necessario aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono raccolti e successivamente trattati, secondo le indicazioni ricevute dal Titolare o Responsabile;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Responsabile;
- mantenere la massima riservatezza sui dati predetti;
- adottare le misure e gli interventi per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati, disposti dal Titolare o dal Responsabile;
- osservare le misure di sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito dei dati personali e in particolare osservare le istruzioni contenute **nell'allegato A)**;
- osservare scrupolosamente le disposizioni organizzative e operative impartite dal Titolare o dal Responsabile per il corretto, lecito, pertinente e sicuro trattamento dei dati custodire e controllare i dati personali oggetto di trattamento in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta;
- accedere ai soli dati personali la cui conoscenza sia strettamente necessaria in relazione e per l'adempimento delle mansioni e dei compiti assegnati;
- accedere, per esigenze di servizio, esclusivamente alle banche dati informatiche del proprio Servizio/Ufficio a cui è stato autorizzato dal Titolare o dal Responsabile;
- segnalare al Titolare o al Responsabile eventuale problemi applicativi rispetto all'attuazione e all'adempimento degli obblighi previsti dal D.Lgs. 196/2003.

Luogo e data _____

Firma del Responsabile del trattamento dati_____

Firma dell'Incaricato/a temporaneo/a al trattamento dati_____

A.S.L. TO5
Azienda Sanitaria Locale
di Chieri, Carmagnola, Moncalieri e Nichelino

Sede Legale – Piazza Silvio Pellico 1– 10023 Chieri (To) – tel. 011 94291 – C.F. e P.I. 06827170017

Allegato A)

ISTRUZIONI PER INCARICATI AL TRATTAMENTO DATI

Il sottoscritto _____ in qualità di incaricato dovrà eseguire le operazioni di trattamento nell'ambito del proprio settore di appartenenza rispettando le seguenti **istruzioni**:

- **distanza di sicurezza**: per quanto riguarda gli operatori di sportello (c.d. front-office) deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- **identificazione dell'interessato**: occorre richiedere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura dei dati anagrafici dell'interessato (nome, cognome, luogo di nascita o residenza) o si voglia avere garanzia dell'effettiva identità del soggetto interessato;
- **controllo dell'esattezza del dato**: fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel proseguo del processo;
- **obbligo di riservatezza e segretezza**: l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;
- nel caso di **consegna di documentazione:** identificare il soggetto interessato, se necessario mediante esibizione di un documento di riconoscimento, al fine di evitare di comunicare dati sensibili a soggetti non autorizzati. Prestare molta attenzione a rilasciare unicamente la documentazione richiesta e autorizzata. Nel caso di trasmissione tramite posta scrivere il destinatario con chiarezza e precisione, al fine di evitare errori che potrebbero causare la consegna del documento ad un soggetto diverso dall'interessato
- **esattezza dei dati comunicati via telefono**: prima di comunicare dati personali l'incaricato deve verificare l'identità dell'interlocutore telefonico formulando, ad esempio, una serie di quesiti per avere certezza di comunicare dati personali a un soggetto autorizzato; deve inoltre fare attenzione all'esattezza del dato che comunica.

Per quanto riguarda l'uso degli **strumenti** del trattamento, l'incaricato deve:

- **telefono**: non parlare mai ad alta voce trattando dati personali per telefono, soprattutto usando cellulari all'esterno dell'azienda o anche all'interno, in presenza di terzi non autorizzati, onde evitare che questi ultimi vengano anche accidentalmente a conoscenza di dati personali altrui. Quando ci si trova in ufficio e si utilizza il telefono fisso utilizzare un tono di voce idoneo ad evitare il medesimo rischio.

  Nel caso di richieste di informazioni telefoniche, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  a. chiedere l'identità del chiamante e la motivazione della richiesta;
  b. richiedere il numero di telefono dell'interlocutore per effettuare le necessarie verifiche sulla provenienza della telefonata

c. accertarsi che la persona che ha richiesto l'informazione sia autorizzata ad ottenerla, perché si tratta, ad esempio, del soggetto interessato, di un incaricato, di organi di amministrazioni pubbliche, o di autorità giudiziarie ecc.

- **macchine fotocopiatrici:** non lasciare accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe.
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  a. digitare correttamente il numero telefonico;
  b. controllare l'esattezza del numero digitato prima di inviare il documento;
  c. verificare che non vi siano inceppamenti della carta ovvero non vengano presi più fogli contemporaneamente;
  d. attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  e. qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  f. in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedono all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: nella duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) l'incaricato deve procedere alla distruzione controllata dei supporti cartacei non occorrenti o non corretti. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere illeggibile il contenuto.
- **supporti di memorizzazione** contenenti dati sensibili o giudiziari: i supporti rimovibili (cd-rom, dvd, chiavette usb, etc..) possono essere utilizzabili garantendo che i dati in essi contenuti siano trattati in modo lecito e non siano accessibili a soggetti non autorizzati. I supporti vanno custoditi con diligenza e il possesso è esclusivo dell'incaricato. Se i supporti non sono più utilizzati vanno distrutti o resi inutilizzabili
- **pc portatili**: sono di facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile e siete stati autorizzati dal responsabile del trattamento dati ad utilizzare un portatile siete tenuti ad adottare tutte le misure idonee per evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali contenuti nel computer, utilizzando, ad esempio, programmi di cifratura del testo rigido.

In tema di **misure di sicurezza** l'incaricato deve attenersi alle seguenti istruzioni:

- **protezione delle aree e dei locali**. Le aree e i locali in cui avvengono operazioni di trattamento dati con o senza l'ausilio di strumenti elettronici devono essere adeguatamente protetti. L'incaricato a cui sono affidati atti e documenti contenenti dati personali deve controllarli e custodirli per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento e impedire che persone prive di autorizzazione possano accedervi. La porta degli uffici va chiusa tutte le volte che ci si allontana per

evitare che un soggetto estraneo o non autorizzato acceda ai dati personali. Alla fine della giornata non lasciare i documenti sulla scrivania, ma chiuderli a chiave in un cassetto o in un armadio o in alternativa chiudere a chiave la porta.

- **trasporto documenti**. Nel caso in cui sia necessario trasportare documenti fuori dall'ufficio o, in generale, all'esterno del luogo di lavoro, l'incaricato deve porre in essere tutte le misure di sicurezza idonee per evitare la distruzione, il furto, la perdita, anche accidentale, l'accesso non autorizzato ai dati contenuti nel documento o il trattamento non consentito o non conforme alle finalità svolte. L'incaricato deve evitare che un soggetto terzo non autorizzato possa visionare anche solo la copertina o le buste di documenti che si trasportano.
  E' proibito portare all'esterno del posto di lavoro fotocopie non riuscite o carta di recupero, da utilizzare altrove per appunti.
- **Parola chiave o password:** La parola chiave, assegnata a ciascuna incaricato, è composta da almeno otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema. La parola chiave assegnata è modificata dall'incaricato al primo utilizzo e successivamente con cadenza almeno trimestrale. Non deve contenere riferimenti agevolmente riconducibili all'incaricato e dovrebbe essere generata senza un significato compiuto (deve essere difficile da indovinare). L'incaricato nello scegliere la propria password deve utilizzare anche caratteri speciali e lettere maiuscole e minuscole. La parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata, comunicata a terzi o ceduta ad altri incaricati. L'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui è titolare. Nel caso di sottrazione o smarrimento l'incaricato deve darne immediata comunicazione al responsabile del trattamento dati per evitare rischi di trattamenti illeciti.
- **Credenziali di autenticazione** di programmi specifici: all'incaricato possono essere assegnate una o più credenziali di autenticazioni che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o insieme di trattamenti effettuato con strumenti elettronici. Egli è tenuto a custodirle garantendo la relativa segretezza. Le credenziali di autenticazioni non utilizzate da almeno sei mesi sono disattivate, salve quelle preventivamente autorizzate per soli scopi di gestione tecnica. A tal proposito l'incaricato in caso di trasferimento, cessazione o di una lunga assenza comunicherà al responsabile il non utilizzo delle password affinché si adottino gli opportuni provvedimenti in accordo con l'amministratore di sistema. I profili di autorizzazione sono individuati e configurati in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento nell'ambito del proprio settore di competenza. Periodicamente viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. Qualora l'incaricato rilevasse anomalie nelle procedure di autenticazione e accessi a dati in violazione a quanto previsto dal Codice Privacy e alle presenti istruzioni è tenuto a darne immediatamente comunicazione al responsabile del trattamento dati o al titolare. Nel caso di sottrazione o smarrimento l'incaricato deve darne immediata comunicazione al responsabile del trattamento dati per evitare rischi di trattamenti illeciti.
- **Protezione computer (sceen-saver)**: in caso di assenza, anche temporanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screen-saver) dotato di password, ovvero di uscire dal programma che si sta utilizzando, ovvero, in alternativa, occorrerà porre la macchina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

- **Back-up:** salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale all'effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati messi a disposizione dell'incaricato. I supporti contenenti le copie di salvataggio devono essere consegnati al soggetto nominato e incaricato della conservazione, ovvero riposti in un contenitore al quale possano accedere solamente soggetti autorizzati.
- **Antivirus**: sono adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus. L'incaricato è tenuto ad evitare i seguenti comportamenti che costituiscono rischio di virus:
  a) Installare programmi provenienti da fonti non ufficiali;
  b) Scaricare dati o programmi da internet;
  c) Copiare dati da supporti di memorizzazione infettati
  d) Aprire mail di dubbia provenienza
  e) Rispondere a messaggi che invitano a "catene di S. Antonio" e simili

  Eventuali situazioni di rischio vanno immediatamente segnalate all'amministrazione di sistema o al responsabile del trattamento dati.

All'incaricato Sig./Sig.ra _____ per svolgere le attività di propria competenza sono state assegnate credenziali di autenticazioni per accedere alle seguenti banche dati e/o programmi informatizzati in uso in azienda:

_____
_____
_____
_____

Firma del responsabile del trattamento dati _____

Il sottoscritto incaricato Sig./Sig.ra _____ dichiara di aver preso visione di quanto sopra e si impegna a seguire le istruzioni impartite

Data e firma dell'incaricato al trattamento dati _____

Allegato 2

ALLEGATO DET. N. 362 DEL 08 GIU. 2011

NOMINA del RESPONSABILE ESTERNO

- Tutti i Direttori di Struttura Complessa sono delegati a formalizzare la nomina del Responsabile esterno, utilizzando il modello predisposto che si allega.

- Sono Responsabili Esterni del trattamento dati tutti i soggetti esterni che effettuano operazioni di trattamento di dati personali e/o sensibili, necessarie per l'esecuzione degli obblighi derivanti da un rapporto giuridico intercorrente con l'ASL, con l'impiego di sedi, attrezzature e personale esterni all'ASL;

- Occorre predisporre due originali del modello, completandoli nelle parti mancanti, dove occorre indicare in ordine:

    1. il nome della Società o Ditta
    2. la sede legale;
    3. la determinazione con cui è stato affidato il servizio;
    4. tipo di servizio che la Società o Ditta svolge per l'ASL
    5. il numero della scheda del Regolamento Regionale per il trattamento dei dati sensibili e giudiziari, approvato con D.P.G.R. 11 maggio 2006, n. 3/R, e pubblicato nell'area riservata alla Privacy del sito aziendale. Il numero della scheda consente il rimando del trattamento dei dati effettuato dal Responsabile esterno al riferimento regionale. Se il trattamento non è previsto dal Regolamento Regionale, indicare una sintetica descrizione del medesimo. In caso di incertezze rivolgersi al Gruppo di lavoro "Privacy".

- Firmare due originali dell'atto di nomina e farli sottoscrivere dal responsabile esterno.

- Un originale verrà trattenuto dal Responsabile esterno e uno conservato dalla Struttura Complessa, responsabile del procedimento. In caso di ispezioni del Garante della Privacy, tale documentazione dovrà essere esibita.

- Trasmettere via e-mail alla S.C. Affari Generali e Legali copia PDF dell'atto di nomina del Responsabile esterno, con cadenza semestrale.

ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DATI

La Ditta/Società _____ con sede in _____ alla quale l'ASL TO5 di Chieri ha affidato con determinazione n. _____ del _____del servizio di _____ è nominata ai sensi e per gli effetti dell'art. 29 del D.Lgs 196/03 RESPONSABILE del trattamento di dati necessari all'adempimento del contratto di cui sopra.

Nell'effettuare le operazioni e i compiti ad essa affidati, che risultano espressamente dagli atti contrattuali, la ditta/società si impegna ad osservare le norme di legge sulla protezione dei dati personali e il Regolamento per il trattamento dei dati personali sensibili e giudiziari, approvato con D.P.G.R. 11 maggio 2006, n. 3/R e, in particolare, la scheda n. _____ relativa al Trattamento "_____". Si impegna altresì ad attenersi alle decisioni del Garante dei dati personali e dell'Autorità giudiziaria, provvedendo ad evaderne le richieste.

La Ditta/Società dichiara di aver adottato tutte le misure di sicurezza predisposte per evitare rischi di distruzione e perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, tutte descritte negli atti contrattuali e nella normativa richiamata. La Ditta/Società si impegna altresì a consegnare alla ASL estratto del documento programmatico sulla sicurezza relativo al servizio di che trattasi e i relativi aggiornamenti.

In ogni caso la ditta/Società si impegna espressamente a non effettuare operazioni di comunicazione e diffusione dei dati personali sottoposti al trattamento verso soggetti terzi diversi dall'azienda committente senza preventivo consenso dell'azienda stessa, non rientrando tali operazioni tra quelle affidate alla ditta.

La Ditta/Società dichiara che tutte le persone fisiche che interverranno nelle operazioni di trattamento hanno ricevuto una formazione adeguata all'incarico affidato.

Chieri,

Il Direttore
della S.C. _____
Delegato dal Titolare del Trattamento
*con deliberazione n.*_____ *del* _____

Il Legale Rappresentante della Ditta/Società