Chapter 11
Towards Trust and Governance in Integrated Health and Social Care Platforms

William Buchanan, Christoph Thuemmler, Grzegorz Spyra, Adrian Smales and Biraj Prajapati

11.1 Introduction

The way we are sharing health and care data will be changing considerably over the years to come. One of the reasons is an increasing move towards patient-centric approaches where services are built around the citizens, rather than citizens integrate with the existing health and social care system. Often our health and social care services have evolved as separate entities where data around the citizen cannot be shared in a structured, safe and secure manner, and thus we often have non-integrated care systems. This lack of integration in the United Kingdom (UK) and in many other countries involves a lack of sharing between primary and secondary health care, but also spans to social care and relevant third sector organisations.

The healthcare domain and the inter-domain space between healthcare and relevant third party domains such as social care are high-risk area for data sharing. Healthcare data are notably the most desired data by hackers which are valued 10 times the value of credit card information on the black market [1]. There is an increasing requirement for strong cybersecurity practices, such as for cryptography

W. Buchanan (✉) · C. Thuemmler · G. Spyra · A. Smales
School of Computing, Merchiston Campus, Edinburgh Napier University, Edinburgh, UK
e-mail: w.buchanan@napier.ac.uk

C. Thuemmler
e-mail: c.thuemmler@napier.ac.uk

G. Spyra
e-mail: G.Spyra@napier.ac.uk

A. Smales
e-mail: a.smales@napier.ac.uk

B. Prajapati
The Hut Group, Northwich, UK

C. Thuemmler and C. Bai (eds.), *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*, DOI 10.1007/978-3-319-47617-9_11

and strong access control. The roles and services, though, have often been developed for health care systems which only have local significance, and lack any integration with external systems. There is thus a requirement for strong governance and security for the sharing and aggregation of data across systems, networks and domains in order to operate data sharing in full compliance with existing national legislation thus protects the rights of patients, organisations and citizens.

The rise of Cloud Computing has helped to make computer resources scalable and available when and where needed. Virtualisation has provided a new method to decouple data from services and servers. These strategies taken together may simplify data sharing across agencies in the future.

The use of global health data is not limited to the care of citizens but is also of huge relevance in a public health context and for governments to analyse the dynamics of the health and social care systems. There is also a vested interest by academics and researchers, for example in the pharmaceutical industry, or with regards to the development of smart algorithms to access real patient data for R&D purposes. However, these desires by different stakeholders need to be carefully balanced with the patients' privacy rights. Recent court rulings in Europe have clearly demonstrated that data sharing practices which were believed to be compliant with legislation and thus fair might after all be not safe and in line with existing legislation [2]. New Governance strategies have to be established to restore trust in order to allow for data sharing with confidence for all stakeholders.

Social and technical issues are to blame for the slow adoption of digital health in the UK and Europe (Fig. 11.1).

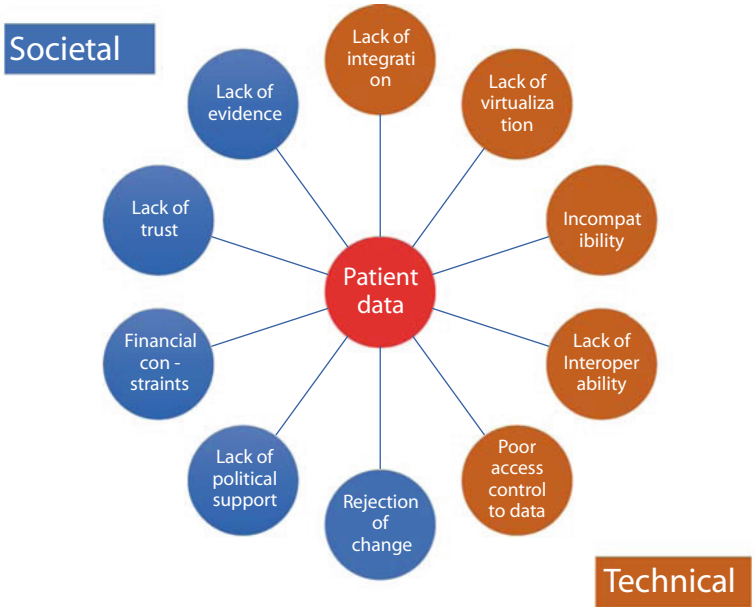

Fig. 11.1 Technical and societal barriers to the adoption of integrated e-Health platforms

Typically the target of integration across platforms, domains and systems is the improvement of the functionality of the existing platform components and the creation of new services. Data users frequently label the following attributes as desirable:

(a) More integrated and cost effect. This will allow inter-agency and collaborative work.
(b) More scalable and flexible.
(c) Better patient care. Support for patient history.
(d) Support sharing of resources.
(e) Reduced costs.
(f) Better quality. This includes generic quality metrics.
(g) Support research. This supports the analysis of data.
(h) Support national security. This helps with the monitoring of the spread of infectious diseases and/or other disease outbreaks, and look at infection patterns.
(i) Support strategic planning. This allows for analytics across the platform.
(j) Support financial operations. This supports the brokering of costs across the platform.
(k) Facilitate clinical trials.
(l) Facilitate forming registries. This allows for the targeting of special groups for care and well-being support.

This document will discuss a number of features such as:

(a) The infrastructure will have a strong definition of data owner of every data element, and for the rights of ownership and governance to these elements.
(b) Care, well-being and health care may all be supported within an integrated platform.
(c) All accesses for requires will be logged and analysed.
(d) Data accesses scopes will be limited by policy and scalable but specific access credentials.
(e) Wherever necessary anonymisation and sanitisation will be integrated into services, in order to preserve privacy.
(f) There should be a break-glass feature within the system that allows access to data, based on various risk factors.
(g) On-chip hardware security might be considered for devices such as sensors and smart phones.

11.2 e-Health Platform Features

Many surveys have been carried out around the world in relation to the requirements for use of technologies in the medical field and there can be no doubt that security and privacy are among the most important requirements. Thus, security

and privacy plays a vital role in successful implementation of e-Health and other medical technologies. A survey found out that females and healthy adults are more security and privacy aware compared to the males and ailing elderly [3]. However, from the point of view from healthcare providers and other stakeholders violation of privacy regulation means exposure to litigation and subsequently heavy penalties and compensation on top of the damage to standing and credibility.

Eysenbach [4] has put together 10 e's that characterises e-Health. These 10 e's can also be classed as a requirement for the e-Health system. According to Eysenbach, an e-Health should be efficient, evidence-based and equitable. It should enhance the quality of care and also follow the patient-physician ethics. It should prioritise the education of health care workers via online sources and also enable the exchange of information in a uniform method. Finally, an e-Health should also encourage relationships between patients and health professionals, resulting in the extension of scope of health care beyond the conventional boundaries.

Although patient-centricity is clearly a future proof attribute of healthcare and consequently e-Health systems there are lots of technological challenges that need overcoming if it is to be successfully implemented over the coming years [5]. On the other hand social components such as especially trust and confidence might play an equal if not bigger role. Technological research and development needs to be aligned with specific legislation to clarify requirements, responsibilities and strengthen the rights of citizens with regards to their own data. All of these processes need to be tackled especially with regards to a unified digital single market [6].

Certainly challenging will be the fact that future e-Health systems need to comply with significantly higher standards but on the other hand be more open and available anywhere, at anytime, anyhow [7].

11.2.1 Simple e-Health Model

A simple terminology for e-Health was developed by Löhr [8]:

- Health Professional (HP). A person who delivers health care services, e.g. physician, dentist, pharmacists, etc.
- Health Care Provider (HCP). An organisation that provides services of health professionals, e.g. doctor's practice or hospital.
- Personal Health Record (PHR). A database of medical data objects and health-related data managed by a patient.
- Electronic Health Record (EHR). A database of medical data objects and health-related data managed by health professionals.

For a simple PHR model, as illustrated in Fig. 11.2, the citizen controls access to the PHR, and grants rights for a HCP to access it.

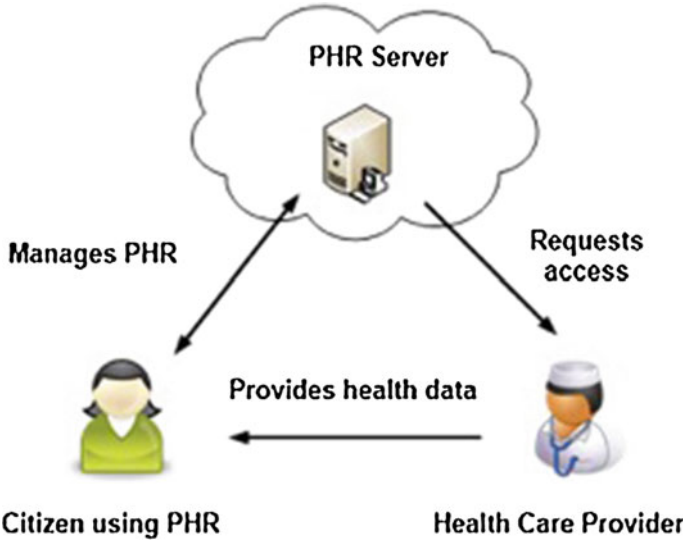

Fig. 11.2 Simple e-Health PHR model

11.3 Interoperating and Integrating Data Across Traditional Boundaries

For an enhanced model of health care, an interagency approach normally supports data to flow around the citizen, and for various care roles to interact, and look more holistically at individuals. Traditional health care systems within the public sector, though, have been built to support only internal accesses, and often fail to properly integrated less trusted access, such as within a home environment or with 3rd sector integration. The major challenge for new health and well-being care models is thus how to integrate systems across a number of domains, without significantly increasing the complexity but ensuring the same or enhanced level of security. This is especially challenging when considering the impact of any system alteration on warranties given by vendors with regards to the legacy system. From a legal perspective there are also issues where rights and identities flow across the different public sector agencies, and then out into even less trusted environments. Many government initiatives have tried to create common identities, but these often fail because they are too complex or citizens do not trust them. The method of BYOI (Bring Your Own Identity), Device/Location Authentication, Biometric Authentication and Multifactor authentication are now commonplace in supporting a more credible approach to identity provision.

Within patient-centric health and well-being systems the focus has to be on the patients and their formal and informal carers, their requirements and their multimodal interactions. This normally involves care services which integrate across different agencies, along with integrating the citizen and their trust circle. In order to

protect privacy and reduce the exposure to data breaches, the core health care data must routinely be kept within highly secure environments and under the control of the patient. However, where there is proper justification, there is a need for those external to a domain to have access to information, following due process.

This has to go hand in hand with a clear understanding of the risks resulting from the progressive use of cyber-physical systems which are based on real time connection of the real, physical and the virtual worlds. Here the risks are less associated with the break in into data bases but the interference with network infrastructures to intercept real time data communication. The different risk categories have been covered in more detail by Kashif Saleem and Ziyuan Tan in Chap. 12 in this book.

There are, of course, many different levels of risk within health and social care platforms. Within a data centre, we have different available requirements for the various tiered levels:

(a) Tier 1. Uses a single non-redundant distribution network path for equipment, and with an availability of greater than 99.671 %.
(b) Tier 2. Improves Tier 1 with redundant site infrastructure components/network connections, and with an availability of greater than 99.741 %.
(c) Tier 3. Improves Tier 2, but has multiple independent distribution paths with dual-power supplies, and an availability of greater than 99.982 %.
(d) Tier 4. Improves Tier 3, but with cooling equipment, dual-powered, with chillers/heater, ventilation and air-conditioning (HVAC). A longer term power outage will normally allow the infrastructure to continue to run, and an availability of greater than 99.995 %.

Normally, the security levels for the different tiers will increase, with Tier 4 data centres having strong security requirements.

11.4 Human and Digital Trust

One of the major challenges within integrated health and social care these days is the building up of both—digital trust and human trust (Fig. 11.3). The challenges in digital trust are the proving of identities of machines and individuals, their roles, and how that maps to the rights of access to the data. To provide a secure environment, all access to

Fig. 11.3 Integration of digital and human trust

data should be disallowed, unless it is explicitly allowed by a defined policy. This policy rule might relate to legal purposes, such as a static rule that allows the GP of a citizen to have access to their health record, or it might be dynamic where it is created by the citizen to allow access to part or all of their patient health record (PHR). The major issue within digital trust is the difficulty in properly mapping identities and rights onto the security parameters within IT systems.

A more serious issue relates to human trust, where few people actually trust the health and social care infrastructure to protect their privacy and rights. Along with this, the adoption of digital services within health and social care will only happen with applications which are useful for health and social care professionals.

However, this does not sit comfortably with a massively increasing trend towards self-monitoring and self-management. Far more than 100,000 e-Health applications are currently on the market globally, most of them not standardised and far beyond the security levels required by health care providing organisations. One of the prominent challenges of the coming decade will be to integrate these applications and a variety of patient-owned smart devices into a framework without creating any additional challenges with regards to responsibility and liability. Alongside new security technologies this will also require new risk management strategies in order to establish the notion of "trust" end-to-end across different networks and domains.

11.4.1 Cross-Domain "Trust" Through Translation Gateways

Within an integrated health and social care infrastructure data should be kept within the domain which governs the citizen's record—the data governor—and which is

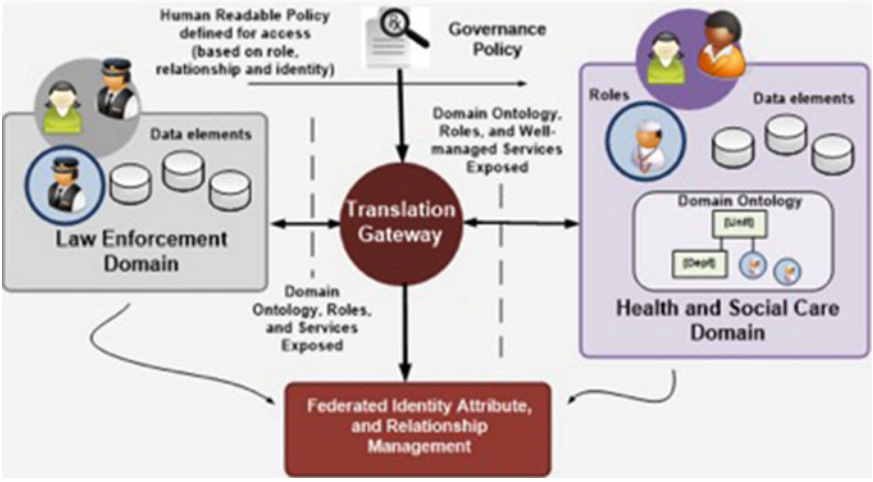

Fig. 11.4 Interdomain rights and mapping

trusted by all stakeholders to control access. All accesses from inside and outside the domain must then be controlled. This requires the mapping of the roles and rights from one domain into another domain. The most secure way to do this is through a translation gateway, which knows the structure of each of the connected domains, and can then check the access requirements for a role or individual from one domain to access a data within another domain. The two domains thus require a common language for the definition of the entities they are referring to, and the levels of identity provision that is required (Fig. 11.4).

The "Translation Gateway" supports a highly safe and secure digital interdependency which could be understood as an equivalent of "trust" in human interaction. The rights of access are defined by predefined rules. Along with this, it uses trusted identity verifiers, so that users can identify themselves in a secure way. Key features of the governance infrastructure are:

(a) Automated governance policy generation from the model.
(b) Ability to produce a human readable version of the information sharing policy, which maps directly to the agencies.
(c) Ability to change the policy in real time, in order to deal with changing environments.

11.5 Trust and Governance

One of the challenges of generic to multi-agency data sharing, such as integrated health and social care information, has been to agree how and what information should be shared across boundaries, without increasing risk and exposure. Traditionally this is solved by using a Master Data Management system which can manage the "trusted" exchange of massive amounts of data between agencies. This type of approach allows for a direct access method in order to "share" information, without actually permanently moving any data—thus keeping information where they are best maintained and managed but at the same time providing rich composite views of information. The system operates by translating the multi-agency model into a human readable policy, which defines the roles and rights of access to information from each of the agency partners. At any time the model can be updated, which, after a review, can be implemented within the translation gateway. The governance policy will then control the access to information between the agencies, in real time. Trust and governance promotes a sharing architecture across agencies, and then defines the information sharing governance policy between the domains. It thus translates identities and rights across the domains within the care of citizens, but where the data in each domain is carefully managed. The benefits are clear for organisations across both public and private sectors:

(a) Ability to share information securely within or across domains.
(b) Strong governance framework to prevent unauthorised access.
(c) Adherence to compliance and policy standards through strong governance framework.
(d) Prevention of cybercrime and more effectiveness and efficiency in cybercrime investigations.
(e) Collaboration between organisations enabling improved joint development and research.
(f) Reduced cost and risk through efficient, robust, secure architecture.

11.5.1 Trusted Identities

Once a governance model is in place we can have a complete provision of the services and roles exposed by each of the managed domains, and then control the access between them. At any given time the rights can be revoked. The governance layer thus just needs to sit as a service between each of the domains. This needs to be the only way to access a given domain in the sense of a single point of contact (SPOC). Just like a network firewall, it will block accesses which do not have the correct access requirements.

A user wanting to access an exposed health care service, such as viewing their child's immunisation record, would thus access the gateway of the domain exposing the service, and then present their credentials and required information of the scope of the request (such as the ID of the child, their relationship to the child, and the dates required). The system then would check its policy for access, and define the identity provision that is required. This will include defining the range of identity providers that the domain trusts, and other specific identity information required (such as a proof of being in a certain location or biometric information). The claim is then checked by a trusted entity to check that it has been signed correctly. If the requirements are met and all features of the request match the policy the access is allowed, and the service runs the query. Throughout the process a complete audit trail is kept for both successful and unsuccessful accesses.

Alternative or additional strategies would be the use of Blockchain technology. Here the access history is irrevocably linked to the data as a metadata tag. This strategy has been proven in the finance domain and might be used in the future to tighten security in the health domain further. This would especially enhance security with regards to the increasing amount of patient devices and e-Health applications.

11.6 Aggregated Records

Increasingly a major barrier for integrated care is to allow care agency partners, such as from healthcare, social care, and education to share information, and thus to allow trusted entities to access summary records or metric indicators. The usage of summary

records and metric indicators thus protect the original data, but allows formal and informal carers to make informed decisions around associated risks.

11.7 Information Sharing

A key aspect for the future of health and social care is the integration of a wide range of health care services within an integrated infrastructure. An important area for information sharing is within the holistic care, where information from different public sector agencies, for example from the health and social care domain can be used to improve the effectiveness and efficiency of care of citizens.

The UK Government and Caldicott [9] have both identified that key objectives of a modern health and social care information is for an improvement information sharing across the public sector, and increased integration of the citizen, and their formal and informal carers, into their health and social care. In this way citizens are more likely to take more ownership of their own healthcare, with an expected improvement in treating illnesses. Unfortunately most health and social care IT infrastructures in the UK have been designed with little thought of integration. Future systems must be built around the citizen, in which we move into holistic care, and where the health and social care professionals integrate with the citizen. This distributes their care, supports the virtualization of care into patients' homes, thus offering a digital infrastructure to empower people to manage their own (chronic) conditions and reduce hospital admissions.

11.7.1 Related Data Architectures

As part of the development of an integrated approach to health and social it is important to analyse current defined architectures, and understand their operation. The data within an e-Health platform will typically only be used internally to the infrastructure, but there will be external interfaces where citizens can access open dataset.

11.7.1.1 London Digital Programme

As part of Healthy London initiative [10], the Health and Social Care ecosystem in London is piloting new ways to provide a data sharing environment to allow the 7000 diverse organisations involved in patient care to access patient records. Symphonic Software is delivering the key governance layer to this important programme to ensure that any data access meets with data controller agreements, which codify the inter-organisational rules for patient data access, and also allowing citizens to express their own data sharing preferences [11]. There are a number of agencies that inter-connect, and the span of the integration of health and social care services [10]:

(a) 9 million people.
(b) 25 miles wide, 25 miles deep.
(c) 1500 GP practices.
(d) 1500 Dental practices.
(e) 1800 Pharmacies.
(f) 400 Opticians.
(g) 30 NHS Trusts.
(h) Hundreds of formal and informal care organisatons.
(i) 32 CCGs and 32 Councils.

11.7.1.2 NIB Framework

The NIB Framework [12] sets out an ambition for the delivery of digital care accounts. The Citizen Accounts project aims to deliver the technical solution design, via follow-on projects, and will support the transformation in the way information is used across health to deliver radical transformation in a number of key areas. Within this broad framework, the Citizen Accounts project explores the requirements and feasibility of establishing personalised identity, consent and preference services that can be set (by the citizen) once and subsequently be accessed/shared by provider systems. The key elements of the integration include covering a number of interlinked use cases supporting the data controller's role and the capture of patient preferences and consent in a platform which provides capabilities against a number of key themes:

(a) Creating data sharing agreements between data controllers, and defining the embodied data rules electronically.
(b) Providing a 360-degree audit view on the creation and use of these data rules.
(c) Providing assurance on identities of patients, clinicians, and 3rd party applications/services making data requests.
(d) Providing an API integration to make it easier for 3rd party applications to conform to the data sharing rules within the electronic platform.
(e) Providing flexible capability to restrict data, including personally identifiable patient data, according to those rules.
(f) Capturing and enforcing patient preference and consent.
(g) Notification services which can be used to inform data controllers of patient preferences.

11.7.1.3 London DataStore

The London DataStore provides access to city-related data [13], and which has the mission statement of [14]:

> We want London to have the most dynamic and productive City Data Market in the world. In our City Data Market, the capabilities, talents and capacity of all our city data partners

> will impact on our huge social, economic and service-based challenges. To make this happen, friction in the sharing and value-driven exploitation of city data will be reduced to a minimum. City data will be recognised as part of the capital's infrastructure. We will use it to save money, incubate innovation and drive economic growth. And London will achieve global renown for data impact.

It integrates data across the city and provides planners with trends which break down in boroughs and wards, and includes a wide range of health and social care services, including data around abortion rates for under 18s, loneliness ratings, and drug and alcohol usage. At present it has over 500 datasets which can be cross-referenced with the required linkage. An important factor is that there is great detail in demographic differences across the city, and each ward and borough can be analysed in great detail for its demographics and changes in its future requirements.

Within [14], the authors define that a major drawback in allowing data to flow is the architecture used, and there is a strong need for regulation and governance, along with culturally and organisational barriers, but that there were so many opportunities for the creation of new skills and jobs. They propose the following design guidelines:

(a) Use a federation of data stores/warehouses. This approach distributes the data, but aims to use an integrated security infrastructure to secure the data.
(b) Focus on cloud-based methods.
(c) Integrate new datasets, such as related to sensor data for IoT access.
(d) Reference data rather than duplicate it.
(e) Support active exchange of knowledge across the public sector in the UK, and elsewhere.
(f) Use and contribute to the open source community.

The initial phase is Phase 1—City DataStore, where there are static and non-standardised data files, along with published API calls for data. The second phase involves the integration of simple API calls, and identity solutions around security, data types, federated data stores, and for federated identity checking. The stages which follow include:

- City DataStore—Phase 3. This will include licensing models and full API integration and identify dataset with the greatest potential for commercial models.
- Data for London—Phase 4. This will include the integration into the WITAN and the Sharing Cities project, along with new tools for open data analysis and visualisation.
- Data for London—Phase 5. This will integrate data from a wide range of platforms.

References

1. Reuters Technology News (2014) Your medical record is worth more to hackers than your credit card. http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924. Accessed 24 Sept 2016
2. European Court of Justice (2015) The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. Press release No 117/15. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. Accessed 1 Sept 2016
3. Wilkowska W, Ziefle M (2012) Privacy and data security in e-Health: requirements from the user's perspective. Health Inform J 18(3):191–201
4. Eurostat (2014) Available via Eurostat: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises. Accessed 19 Jan 2015
5. Armstrong D, Kline-Rogers E, Jani SM et al (2005) Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome. Arch. Internal Med 165(10):1125–1129
6. European Commission (2015) Digital single market: digital economy and society. https://ec.europa.eu/digital-single-market/en/eu-policy-ehealth. Accessed 24 Sept 2016
7. AbuKhousa E, Mohamed N, Al-Jaroodi J (2012) E-Health cloud: opportunities and challenges. Future Internet 4(3):621–645
8. Löhr H, Ahmad-Reza S, Marcel W (2010) Securing the e-Health cloud. In: Proceedings of the 1st ACM international health informatics symposium, ACM
9. UK Department of Health (2012) Information: to share or not to share? Information governance review. http://caldicott2.dh.gov.uk/. Accessed 1 Sept 2016
10. Part M (2016) The London digital programme. http://digitalhealth.london/wp-content/uploads/2016/03/Mike-Part-London-Digital-Programme-2.pdf. Accessed 1 Sept 2016
11. Delfs H, Knebl H. (2007) Symmetric-key encryption. In: Introduction to cryptography. Springer, Berlin, pp 11–31
12. HM Government (2014) Personalised health and care 2020 NIB framework. Available via https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384650/NIB_Report.pdf. Accessed 1 Sept 2016
13. Mayor of London (n.d.) Developing data infrastructure for London. http://data.london.gov.uk/blog/developing-data-infrastructure-for-london/. Accessed 1 Sept 2016
14. Suzuki LCSR (2015) Data as infrastructure for smart cities. PhD Thesis, University College London. http://www0.cs.ucl.ac.uk/staff/l.romualdo/DataInfraForSmartCities/. Accessed 26 Sept 2016