IoT in Health and Social Care

Preserving Privacy: Good Practice Brief

NOVEMBER 2017

Produced by
Contents

Introduction ................................................................. 3
The DASH Project ............................................................ 4
Why the Need for Guidelines? .............................................. 5
The Guidelines ................................................................. 6
  DASH ethical principles for H-IoT design ....................... 6
  DASH ethical guidelines for H-IoT design ...................... 6
  Table 1 - Relationship between principles and guidelines .... 7
SeNTH – Security & New Threats in Healthcare ...................... 8
Challenges ................................................................. 9
Introduction

With recent advances in technology and more favourable patient attitudes, health-related Internet of Things (H-IoT) has the potential to further flourish in the coming years. Better product design - including miniaturisation of sensors and smaller batteries, alongside regulatory environment on personal data sharing and ubiquitous internet access, have been other contributing factors to the expansion of H-IoT. H-IoT has already been playing a growing and significant role in health management in both the health and social care setting.

H-IoT provides numerous advantages to citizens, health and care professionals and facilities. These are wide-ranging, from testing of treatments, actuation of medical devices, to wellbeing and fitness monitoring, which is seeing traction in the commercial space with popular apps and wearables. In combination with its numerous applications and benefits of H-IoT, adoption by medical and social care institutions is increasing.

Sensitivity of data sharing and the threat of cyber attacks is, however, a real concern for healthcare providers, industry and the public. Patient data and trust must not be compromised.

As part of NHS England’s Test Bed programme, two Internet of Things (IoT) Test Beds - Diabetes Digital Coach in the West of England and Technology Integrated Health Management helping people with dementia in Surrey – have brought innovators, the health system, and academia together to produce guidelines on the collection of data from H-IoT devices.

The Test Beds Programme was initiated by NHS England and the Department of Health in January 2016 to benefit patients with a range of health conditions and improve the way NHS services are delivered, including through using new technologies. Collaboration, particularly on legal and ethical issues, provides the backbone to the future success of the Test Beds.

The PETRAS Internet of Things Research Hub is a consortium of nine leading UK universities researching issues in IoT privacy, ethics, trust, reliability, acceptability, and security.
The DASH Project

An example of guideline development is the recently completed University of Oxford research project as part of the PETRAS IoT Research Hub: DASH - Data Analysis in IoT Solutions for Healthcare. The project suggests nine principles and guidelines for ethical design of the health-related Internet of Things.

This project, with feedback from the two IoT NHS Test Beds, has created ethical guidelines and principles to guide in the use of health data collection.

Devices used in health and social care IoT will be collecting data about patients and customers to inform clinical teams and social workers among others about a range of different aspects of the person’s life to improve health outcomes and support medical staff. This data collection needs to be compliant with all relevant data protection laws, National Data Guardian Guidelines and other good practice guidelines.

DIABETES DIGITAL COACH – a project led by the West of England AHSN in partnership with Diabetes UK and technology companies including Hewlett Packard Enterprise. Bringing together mobile health self-management tools (wearable sensors and supporting software) with the latest developments in connecting monitoring devices (Internet of Things), the Test Bed will enable people with Type 1 or Type 2 diabetes to ‘do the right thing at the right time’ to self-manage their condition. It will also encourage more timely and appropriate interventions from peers, healthcare professionals, carers and social networks.

TECHNOLOGY INTEGRATED HEALTH MANAGEMENT (TIHM) – a collaboration between Surrey and Borders Partnership NHS Foundation Trust and an array of health technology providers which will help people with dementia to live in their own homes for longer. Individuals and their carers will be provided with sensors, wearables, monitors and other devices, which will combine into an ‘Internet of Things’ to monitor their health at home. This will empower people to take more control over their own health and wellbeing, as well as enabling health and social care staff to deliver more responsive and effective services.
Devices used in health and social care IoT will be collecting data about patients and customers to inform clinical teams and social workers among others about a range of different aspects of the person’s life to improve health outcomes and support medical staff. This data collection needs to be compliant with all relevant data protection laws, National Data Guardian Guidelines and other good practice guidelines.

Why the Need for Guidelines?

The National Cyber Security Centre in their 2017 report *The Cyber Threat To UK Business* said of cyber threats: “The threat comes from internet-connected devices, part of the ‘Internet of Things’ (IoT), that are vulnerable to remote code execution or remote takeover. Many connected devices have been shipped with less secure software and default passwords.”

Data security is a particular concern in health and social care where personal data from wearable and implantable devices increase risks of breaches of privacy and potential for hacks. Risks for the individual citizen include potential physical harm, hackers accessing other personal devices and loss of protected health information. Recent technological advances, low user awareness of risks, and the rise of “cybercrime as a managed service” all heighten the risks.

A cultural shift is occurring, in which people used to social networking and commerce are open to sharing their data, if they get more personalised information and advice on their health or behaviour in return. This also requires that organisations are open about what they are doing with the data.

To complicate matters, H-IoT data is more useful if shared with clinicians, and sometimes only reaches its full potential if shared again with third parties, such as research bodies or public health organisations.

The inherent success of H-IoT is rooted in the trust and goodwill of the users and clinicians, as well as friends, family and carers of H-IoT users. Citizens, particularly as patients, can face a challenge retaining control over their data due to the scale, scope and complexity of systems that create, aggregate, and analyse personal health data. The inherent sensitivity of health-related data being generated and the security risks associated with connected devices require careful management, including but not only compliance with the General Data Protection Regulation. There is also a role for voluntary guidance to help ensure good practice and that citizens are protected and reassured.

DASH was an extensive literary review in combination with biomedical big data, looking at health related IoT, and a narrative review on ethics in big data. The study addressed what issues are most prevalent in recent academic literature. Two focus groups were run in cooperation and support from civil society, think tanks, and academia. The extensive one-year project ended in February 2017.

---

The Guidelines

DASH developed a literary study to summarize the “best in-class” ethical principles and guidelines for H-IoT design. Covering the wide-ranging problems consisting of ethics of devices, data, and practice, the guidelines and principles sum up best-in-class strategies for data integrity.

DASH ethical principles for H-IoT design

1. Respect individual privacy
2. Respect group privacy
3. Collect the minimal data required
4. Maintain trust and confidentiality between H-IoT users and providers
5. ‘Do no evil’ – data collection for good reason
6. Respect autonomy and avoid subtle nudging of user behaviour
7. Ensure data processing protocols are transparent and accountable
8. Embed inclusiveness and diversity in design
9. Facilitate public health actions and user engagement with research via the H-IoT

DASH ethical guidelines for H-IoT design

1. Give users control over data collection and transmission
2. Iteratively adhere to industry and research confidentiality standards
3. Design devices and data sharing protocols to protect user privacy by default
4. Use alternative consent mechanisms when sharing H-IoT data
5. Meet professional duties of care and facilitate inclusion of medical professionals in H-IoT mediated care
6. Include robust transparency mechanisms in H-IoT data protocols to grant users oversight over their data
7. Report the uncertain utility of H-IoT data to users at the point of adoption
8. Provide users with practically useful mechanisms to exercise meaningful data access rights
9. Design devices to be unobtrusive according to the needs of specific user groups

The Technology Integrated Health Management (TIHM) project in Surrey was set up to help people with dementia and their carers. The Test Bed collects continuous monitoring and observation data, which are translated into a common language to provide real-time insights and alerts. This allows local healthcare staff to deliver more responsive, better and effective services and will reduce the burden on carers.

Most of the devices operate in the background in homes, collecting information, following a patient consent process. For example, sensors can measure a person’s movements round the home and identify if they have had a fall. Others, such as weight and hydration scales and a blood pressure cuff, require a person to interact with the device.
A number of the principles outlined above can be seen in operational data management. All data collected has received oversight from clinical teams to ensure only relevant data is collected, and the Test Bed received explicit consent from each patient and their carer, whilst not using personal identifiers. Only dementia patients able to understand the idea of sharing data and privacy were invited to participate. On the healthcare provider side, only those who explicitly need data access have access to it, for example, clinicians.

The devices themselves are not sending patient identifiable data, relying instead on summarisation and generalisation, meaning companies involved - including any third parties - don’t know the identity of the participants with dementia. For a small number of pilot projects that do need an individual identifier, the patients and companies sign up to special contracts to ensure patient privacy. Devices are tested for security weaknesses (penetration testing) so that any vulnerabilities found can quickly be addressed. Contracts are also in place with monitoring and information sharing agreements. Any data that does not need to be passed on to separate systems is retained.

The ethical principles and guidelines are intended to work together. The guidelines serve as grounded advice to embed the ethical concerns incorporated in the principles in the design of H-IoT devices and data protocols.

<table>
<thead>
<tr>
<th>Table 1 - Relationship between principles and guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principles</strong></td>
</tr>
<tr>
<td>1. Individual privacy</td>
</tr>
<tr>
<td>2. Group privacy</td>
</tr>
<tr>
<td>3. Data minimisation</td>
</tr>
<tr>
<td>4. Trust and confidentiality</td>
</tr>
<tr>
<td>5. Non-maleficence and beneficence</td>
</tr>
<tr>
<td>6. Autonomy and nudging</td>
</tr>
<tr>
<td>7. Transparency and accountability</td>
</tr>
<tr>
<td>8. Inclusiveness and diversity</td>
</tr>
<tr>
<td>9. Engagement with public health and research</td>
</tr>
<tr>
<td><strong>Guidelines</strong></td>
</tr>
<tr>
<td>1. User control</td>
</tr>
<tr>
<td>2. Confidentiality standards</td>
</tr>
<tr>
<td>3. Privacy by default</td>
</tr>
<tr>
<td>4. Alternative consent</td>
</tr>
<tr>
<td>5. Duties of care and inclusion</td>
</tr>
<tr>
<td>6. Transparency and oversight</td>
</tr>
<tr>
<td>7. Uncertainty utility of data</td>
</tr>
<tr>
<td>8. Data access rights</td>
</tr>
<tr>
<td>9. Unobtrusive devices</td>
</tr>
</tbody>
</table>
Following on from the work at DASH, the IoT Security for Health Care (SeNTH) project was created by other PETRAS researchers from Imperial College London. The project is currently under way, and aims to develop autonomous security that can be deployed in a healthcare setting within miniaturised devices where computational resources are limited. The project will also investigate fail-safe mechanisms for reliable sensing and data integrity.

These guidelines are relevant for the NHS Test Beds and for businesses investing in H-IoT. For example, TIHM are seeking to bring together organisations to make good use of technology and skills for data security, with a focus on engagement and understanding, alongside legal contracts and technological safety. Academic researchers work closely with public and private sector organisations to develop an understanding of their needs.

**SENTH – SECURITY & NEW THREATS IN HEALTHCARE**

**TEAM:** Guang-Zhong Yang (Imperial College London), Benny Lo (Imperial College London), Emil Lupu (Imperial College London).

This project aims to investigate the security of IoT devices, particularly in the context of implantable and wearable sensors. Key objectives of the project are: (i) to understand how to undertake security process and threat modelling for body sensor networks involving both wearable and implantable devices whilst combining the human, cyber and physical elements (ii) to investigate the security mechanisms that can be provided on low power ASICs combining elements of confidentiality, user control and fail-safe mechanisms and (iii) to establish a Test Bed environment with selected representative scenarios in which novel solutions can be deployed and evaluated.

**Target outcomes:**

An analysis on medical device security threats, including analysis on device resource and security trade-offs for distributed encryption, secure device-user interactions, and possible new algorithms for policy enforcement.

A Test Bed environment for the deployment and evaluation of novel security schemes. This includes a range of sensors (3-4) and medical devices in a realistic deployment scenario. A series of tests and attacks against these systems will also be designed for evaluating the security schemes.
Challenges

As expected, a number of challenges have come up in the work of the Test Beds and the academics’ research above.

● **TECHNOLOGY LIMITATIONS:** H-IoT devices have short range and short communication ranges. It has been crucial at the design stage to develop functionality to preserve continuity if parts of the device or system are hacked.

● **H-IOT COULD REQUIRE REGULATORY CHANGE,** both clinical and technological. Audit functions for continued improvement need to be built into organisational practice within the NHS. Safety measures will encompass standards and practices and regulation. On the management side, Chief Safety Officers’ (CSO) roles are in the process of being developed to include technology as well as clinical responsibilities.

● **SECURITY:** Not surprisingly, security is currently one of the biggest challenges in H-IoT in the view of PETRAS and the NHS Test Beds. The current standards, set by NHS England, aim to help address this. Regulatory bodies, including NHS Digital, are scrutinising devices – any that are accredited for NHS use must be used as part of a viable treatment programme and designed as ‘clinical-grade’.

● **PERSONAL DATA:** Public trust in service and technology service providers could be encouraged by giving people good information on how and by whom their data is used. Trustworthiness is and will continue to be a major issue in H-IoT. Many people want to trust the suppliers. GDPR will help ensure that how information that is collected for H-IoT is used is clearly communicated by those collecting any data.

● **SPREADING AWARENESS:** research and experience from academia and the NHS Test Bed environment can helpfully be shared more widely with organisations and the public, as academic colleagues are doing with DASH guidelines.