ABHI
DIGITAL HEALTH

ABHI WHITE PAPER: DIGITAL HEALTH REGULATORY CONCEPTS

CONTENTS

EXECUTIVE SUMMARY

This paper addresses the regulatory regime for Digital Health Technologies (DHTs), including AI, in light of the EU exit and the move to a UK sovereign regulatory framework for medical devices and diagnostics. In doing so, the specific issues, characteristics and opportunities for Digital Health need to be explored. It also addresses the need for further alignment, clarity and guidance in the regulatory frameworks for data sharing to foster an innovative ecosystem in the highly complex lifecycle of devices, diagnostics and DHTs.

To enable a thriving Digital Health ecosystem a shift to a more nuanced, risk-based, modernised regulatory framework that is swifter, more predictable and transparent is needed. This will reduce the time and cost of market entry and help maintain and enhance the product across its lifecycle to ensure an appropriately streamlined path for increasingly advanced, and increasingly connected, DHTs.

Regulation needs to focus on ensuring that healthcare professionals and users gain, or maintain, timely access to high-quality, safe and effective Digital Health products and services, safeguarding ethical and data protection considerations and balancing them against innovation and speed of access to technology.

Industry has well-established relationships with key regulators, particularly the Medicines and Healthcare products Regulatory Agency (MHRA). The direction of travel signalled by the MHRA looks well-aligned to industry views and we welcome the opportunity to build on this work to collaboratively develop new systems.

A modern regulatory methodology will support faster patient access, improve safety and position the UK as an attractive investment and launch market.

KEY RECOMMENDATIONS

1. Cross-organisational working should be employed to ensure a holistic approach that aligns regulation of product, data and service.
2. Digital Health Technologies should have a distinct and separate approach within the new UK Conformity Assessment (UKCA) process.
3. Develop an agile regulatory framework utilising an appropriate mix, based on risk and level of innovation, of regulation, harmonised international standards, guidance, common specifications and target product profiles, minimising need for legislation.
4. A risk-based classification system is fundamental to the approach and we recommended one closely based on International Medical Device Regulators Forum (IMDRF) principles.
5. A robust nomenclature should be developed to determine the scope of products for which regulation is applicable.
6. Streamline data governance to ensure that data can flow seamlessly across the health system and that industry can access de-identified health data.
7. Provide greater clarity and guidance on use cases and data sharing to address inconsistencies between the common law duty of confidentiality and data protection legislation.
8. Provide legal certainty on issues of product liability, patient redress schemes and safety.
9. The new UK sovereign regulatory process should be implemented with speed, agility and transparency.

INTRODUCTION

Regulation needs to focus on ensuring that healthcare professionals and patients gain or maintain timely access to high-quality, safe and effective digital health products and services, ensuring that ethical and data protection considerations are taken and balanced against innovation and speed of access to the technology.

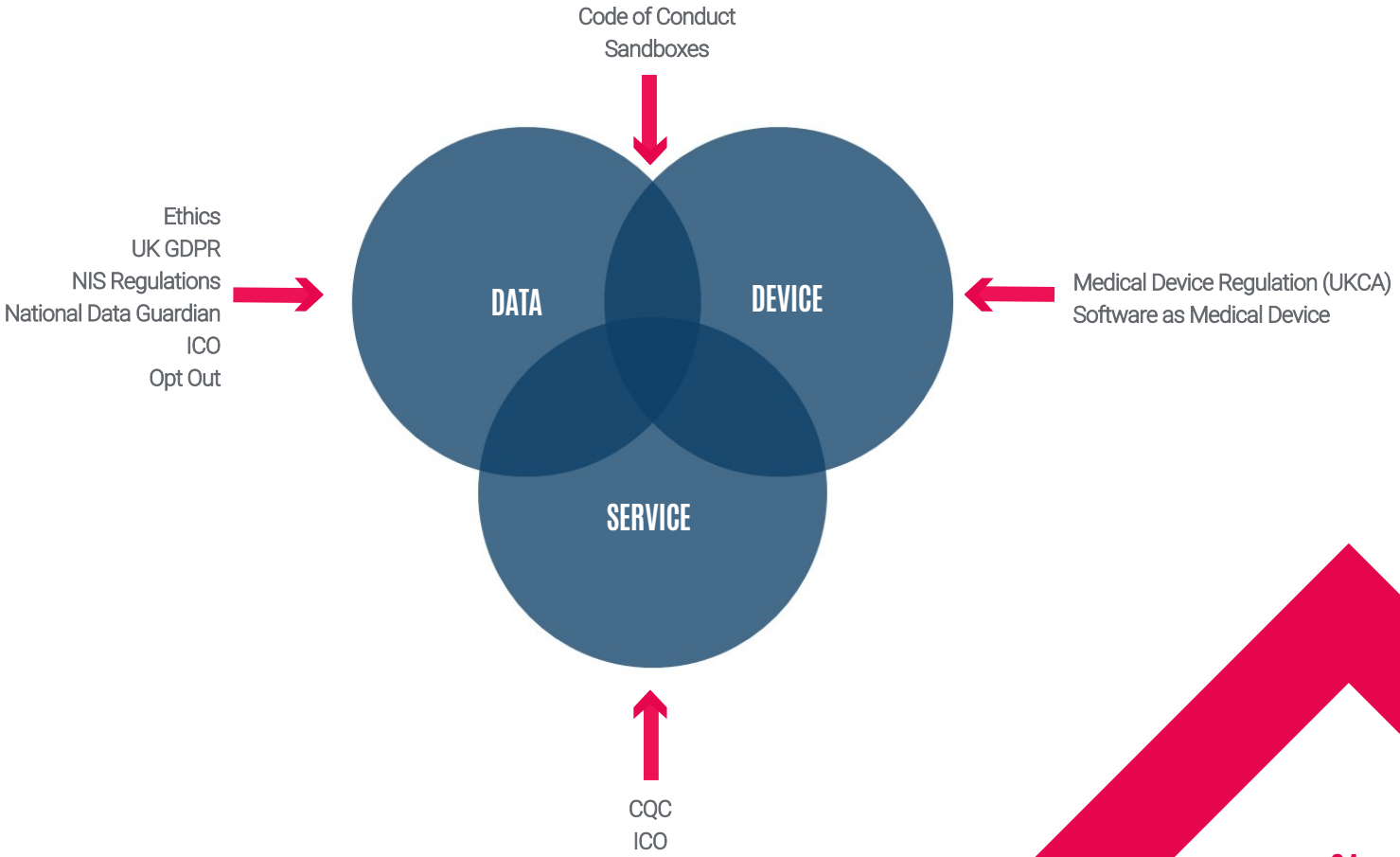
Regulation has as an important role to play in demonstrating to the public, and to users, the trustworthiness of the system to build confidence in the use of data, software and devices as part of health and care delivery.

This paper addresses the regulatory regime for DHTs, including AI, in light of the UK exiting the EU and the move to a legal requirement for national rules and regulations for medical device and data regulation outside of European Directives or Regulations. Attention has focused on the move to the implementation of the UKCA mark by the MHRA, and the opportunities that will provide.

However, it is important to consider the implementation of product regulation in the context of the wider regulatory landscape for deployment of data driven health services. We also highlight the need for further alignment, clarity and guidance in the regulatory frameworks for data sharing to foster an innovative ecosystem in the highly complex lifecycle of devices, diagnostics and DHTs. Further there is also a need to consider the global nature of the health technology industry and inherent need for cross border data flows.

The proposals laid out in this document are for the regulatory framework for DHTs, the related data flows and the service environment in which it functions. This paper will outline recommendations across these three domains:

- **Product**: implications for the proposed UKCA mark.
- **Data**: supporting safe, streamlined industry access to appropriate de-identified datasets and broader use of data for secondary purposes such as scientific research.
- **Service Delivery:** closing the data loop to deliver safe and effective real-world use of DHTs.



Furthermore, we will look at issues that need to align across these domains. The Multi Agency Advisory Service being established by NHSX will have an important role to play in delivery.

When considering DHT regulation we need to do so in the context of issues that have been identified[1] in the broader process, these include:

- No one body/unit is responsible for the overall process, which makes it difficult to ensure coordination between regulators.
- In some specific instances, the current regulation itself is disparate and not fit-for purpose. The letter of the law would require people to go through such cumbersome processes that regulators follow the 'spirit of the law' instead.
- In some cases the remit of regulators is unclear or overlapping, which means that no one, or everyone, is responsible for policing a specific regulatory requirement.
- There are uncertainties about how to regulate certain aspects of AI, such as machine learning.
- Generally, regulation lags behind the technology. When the regulations are made available, the technology has already surpassed the current status that the regulations are intended to control.

PRODUCT REGULATION

Product lifecycles in DHTs are characterised by an agile process where the product is updated at frequent and regular intervals, sometimes multiple times a week. Artificial Intelligence (AI), as an extreme case, takes product iteration to a new level, where 'updates' potentially occur continuously and without human intervention. Continuous innovation in response to changing user demands, new data inputs, operating environments or the need to respond quickly to security vulnerabilities or adverse events drives further rapid updates at a much higher frequency than "traditional" medical devices experience.

To fully align the pace of change in technologies and the regulatory system, it is anticipated that the process of initial and ongoing approval and post market surveillance (PMS) needs to differ from traditional regulatory systems applied to medical technologies.

Scope

The broad scope of Digital Health includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalised medicine.

DHTs use computing platforms, connectivity, software, and sensors for health care and related uses. These technologies span a wide range of uses, from applications in general wellness to applications as a medical device. They include technologies intended for use as a medical product, in a medical product, as companion diagnostics, or as an adjunct to other medical products (devices, drugs, and biologics).[1]

As a pragmatic approach, for the purposes of this document, we will concentrate on product classified as medical devices or diagnostics as defined within the current guidance from MHRA and "Software as a Medical Device" (SaMD)[2].

It is recognised that the demarcation between medical devices and wellness apps can be difficult to define. This necessitates strong cross organisational working between regulators and other bodies such as NHSX and NICE to align formal regulatory systems with processes such as the Digital Technology Assessment Criteria (DTAC) from NHSX and NICE Evidence Standards Framework.

Principles

The programme should be based on overarching principles of:

- **Globalisation**: the process should align with international principles for product and data regulation and be underpinned by international standards, ideally harmonised across leading markets, wherever they support an optimal regulatory framework.
- **Realistic & Equitable**: regulation should be proportionate and appropriate to the classification of the product and/or the risk of the service being delivered.
- **Agile**: the process should enable rapid regulatory review based on clinical risk posed and where appropriate maintain a company's ability to approve changes themselves in line with their Quality Management System (QMS).
- **Creativity**: utilise legislation sparingly and support innovative use of essential standards and guidance within current frameworks.
- **Transparency**: the process should have clear scope, methodology, guidance for use and timelines; it should be open to all companies that meet transparent criteria.

A shift to a more nuanced, risk-based, modernised regulatory framework that is swifter, more predictable and transparent will reduce the time and cost of market entry and help maintain and enhance the product across its lifecycle.

Standards can have a strategic role in providing a faster and more agile route to addressing gaps in the regulatory regime. Utilising international, harmonised standards (IEC, ISO) that can evolve over time, and quickly respond to changes in technology should be the default approach rather than utilising legislation. Specifically, standards for QMS need to allow rapid change in the system to support agility in product lifecycle management.

Structure

Product regulation of medical devices currently falls into two categories, that for medical devices and that for invitro diagnostics, currently DHTs are triaged into one of these two workstreams. We would propose that a third specific and bespoke workstream is developed for DHTs. This will help address some of the specific issues with continuously learning algorithms in high-risk applications:

1. Continuously learning algorithms change the way input information is processed. This may lead to a change to a specific decision of the AI. That means that verification and validation must respond throughout the learning process.
2. Algorithms are sensitive to adversarial attacks, e.g. a small change in the data can destroy the policy of the AI (maybe leading to unpredictable behaviour).

A modern methodology, (building on the 'new legislative framework' [3] to regulation) based on a system specifically designed for Digital Health and AI technologies will be an important factor in making the UK a destination of choice for investment from Digital Health companies and an early launch market for new technologies.

There are two distinct elements to the proposals:

1. Assessment of company values, behaviours and process.
2. Specific product/product line processes and characteristics. Within this there are two but interlinked areas via a feedback loop into continual improvement and risk management:
    i. Process for initial development.
    ii. Post market surveillance and feedback loop for product updates.

Company Accreditation

Building on the approach taken in other sectors[4], or jurisdictions[5], we recommend a more organisational and ethics-based framework, allowing streamlined approaches, while still protecting patients and users, through appropriate, risk-based levels of oversight.

This approach incorporates an assessment of developers' processes, business principles alongside product specific processes. It will assess their ability to manage the product development from inception, through testing, deployment and continuous improvement over the product lifecycle.

This will be underpinned by:

- Compliance with essential standards.
- Verification and validation including cybersecurity and data handling and quality.
- Data Protection.
- Ethical Approach.
- Company culture and business ethics.
    i. Quality management and lifecycle management processes (ISO 13485).
- Supply Chain Management.

Risk Categorisation

Having an appropriately nuanced and structured classification with clear evidence requirements based on risk level is fundamental to ensure patient safety, minimise bureaucracy, demonstrate trustworthiness to the users and assist in error identification.

Outline the risk categorisation for the DHT based on:

- Intended use, medical purpose, functionality and strategy.
- Clinical evaluation and real-world performance.
- NICE evidence standards.
- International regulatory classification[6] as outlined below.

State of Healthcare situation or condition	Significance of Information provided by SaMD to healthcare decision		
	Treat or Diagnose	Drive Clinical Management	Inform clinical Management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

- Detail the "mode of action" for the algorithm and the clinical purpose of the product.
- Clinical strategy aimed at resolving an unmet need that carries a certain level of risk (determined by means of the IMDRF classification).
- Company statement on intended use, outcomes, data flows and mode of action. (Aligned to NHS Code of Conduct Principles 1-7)[7].
- Validation testing based on risk level.
- "Sandbox" testing for highest levels of risk.
- Risk management approach.
- Strategy for data sourcing, curation and quality assessment.

Post Market Surveillance

An approach to Post Market Surveillance (PMS) should incorporate both proactive and reactive elements and processes. Critical to meeting PMS requirements will be timely, possibly real-time, access to relevant data. For rapidly changing high risk DHTs a more frequent review cycle may be appropriate. As laid out above (Data Regulation) changes should be made to the information governance rules to enable access for manufacturers to relevant data. Key characteristics of the process would be:

1. Surveillance and data capture plan:
    i. Use of real world/real time data to determine continued efficacy.
    ii. Capture of health economic data to support value for money and budget impact.
    iii. A post-market clinical follow-up (PMCF) that takes into account the specific intended use of the DHT.
    iv. Adverse incidents: clinical and cybersecurity.
2. Data analysis regime, including assessment of accuracy, completeness and consistency.
3. Version control and mechanism for tracking and distribution of software updates.
4. Governance:
    i. Ethical examination of how data is used. Monitor user reactions to the use of the data-driven technology, and gauge levels of acceptance.
    ii. Commercial model (if relevant, e.g. risk share, equity stake etc.).
5. Risk Management should be incorporated into design change and control, thus making the entire process swifter:
    i. Proactive monitoring for identified risks through seeking user feedback.
    ii. Feedback loop into risk management process from surveillance.
    iii. Use of proactive cybersecurity measures such as "White hat" hacker testing and server resilience.
6. Timely response to events as outlined in IEC 60601-4-5.

DATA REGULATION

The flow of data is important to both the development, training, functioning and on-going monitoring of digital health technology and solutions. Clinical trial data is well monitored under the Data Protection Act 2018 and trial regulations which takes into account use of health data for research. Further guidance is needed to ensure there is an analogous framework to deal with datasets created for post market surveillance and clinical follow-up. This will ensure appropriate access for regulators, users and developers to the data necessary to ensure delivery of safe and effective technologies and their safe implementation within a health, care or wellness context.

There is a particular issue with the inconsistencies between the common law duty of confidentiality and clinical trial legislation and the legal concepts which appear in data protection legislation like the GDPR. These are explored below, with thanks to Baker McKenzie on whose work this is based[8].

Intersecting Regulatory Regimes

This area is complicated by two intersecting regulatory regimes governing the use of health data that are inconsistent with one another, but nevertheless overlap:

- Firstly there is the traditional healthcare regulatory framework, which includes the common law duty of confidentiality and the regulation of medical devices.
- Secondly there are the legal concepts which appear in data protection legislation like the GDPR (and now, the GDPR as incorporated into UK domestic law). The GDPR employs concepts like data controllers and data processors which have been developed and cultivated totally outside the healthcare context, and were originally designed by legislators with quite simple supplier-customer concepts in mind. These 'black-and-white' concepts do not quite work in healthcare, where there are multiple players with nuanced roles, such as healthcare providers, researchers and developers, manufacturers and distributors.

This disconnect (which manifests itself between the NHS and ICO) has been highlighted as one possible reason why the NHS can be overly cautious regarding data sharing[9].

There is huge potential for regulatory guidance in this space to clarify this intersection between these two regimes. Such guidance would need to involve multiple stakeholders, given the interplay of regulatory regimes, including the National Data Guardian, the Information Commissioner's Office, NHSX, the MHRA, and the Health Research Authority (HRA)[8].

Anonymisation

Developers and researchers often request access to 'anonymised' datasets. Thresholds for anonymisation between the GDPR and the common law duty of confidentiality are very different. The 'confidentiality' standard for anonymisation can be conflated with the 'GDPR' standard:

- Truly anonymous information falls outside the remit of the GDPR and its compliance obligations, making it an attractive concept for researchers. However, anonymisation under the GDPR is a high bar and difficult to achieve in practice.
- The GDPR position is more stringent than under the common law duty of confidentiality. Traditionally, researchers in the health space have assumed that removing certain key identifiers will be sufficient to 'anonymise' a dataset for medical confidentiality purposes.
- Often, data considered 'anonymised' for confidentiality purposes are actually 'pseudonymised' data for GDPR purposes. Pseudonymised data may include data where key identifiers have been removed and the data can no longer be attributed to a specific individual without the use of additional information. This additional information must be kept separately and subject to certain technical and organisational measures to ensure non-attribution to any individual. The key takeaway is that pseudonymised data is still personal data subject to the GDPR.

Legal Basis for Data Sharing

This is another area where there are unintended consequences of the two regulatory regimes, as innovators may conflate (a) consents required for confidentiality purposes or for clinical investigations or interventions, with (b) a requirement for GDPR consent. This can often result in stifling innovation as innovators ignore alternative (and less onerous) legal bases for data use that are already available to them under the GDPR. As a result, they are reluctant to maximise the use of their datasets, given that often, GDPR consent has not been obtained.

In the healthcare context, consent may be required for different regulatory purposes:

- Under the common law duty of confidentiality, healthcare professionals may only disclose confidential patient information outside the direct care setting on the basis of consent or certain other statutory grounds. This consent is a relatively low standard of consent, at least when compared to the GDPR.

- Separately, there may also be a regulatory requirement for consent. A prime example is the requirement for the 'informed consent' of clinical investigation participants.

However, this is very different to the GDPR position. Under the GDPR, every processing of personal data requires a legal basis for processing under Article 6. An additional ground is required under Article 9 if processing a special category of data, such as health data or genetic data. It is true that consent appears as a ground under Article 6, and explicit consent is a potential ground under Article 9 of the GDPR. However, the key point is that GDPR consent is one of several grounds which may be available to innovators, even in the life sciences industry.

Recommendations

- Streamline data governance to ensure that data can flow seamlessly and securely across the health and care environment.
- Access to a broad range of data for DHT providers to benefit care delivery and accelerate UK-led innovation.
- Changes are needed to leverage large datasets to improve therapies, conduct scientific research and develop new DHT solutions for the public benefit. A number of mechanisms are proposed to be further investigated:
    i. Issue guidance to support greater use of joint controllership of personal data for the manufacturer/developer (who, typically, has access to that personal data in the capacity of processor, only) in certain clearly defined circumstances.
    ii. Establish a streamlined authorisation/certification scheme to enable access to de-identified personal information for clearly defined secondary use purposes. This will provide an option for developers to overcome multiple, varying application processes.
- Provisions are incorporated in any trading agreements to support the flow of data cross border and that any need for locating of data in national jurisdictions are minimised.
- DHTs may provide the opportunity to demonstrate near real time performance data which could greatly enhance clinical safety and post market surveillance, the recommendations below would be needed to enable this.
- Issuing clear guidance on the thresholds for anonymisation that takes into account both the GDPR and the common law duty of confidentiality. Policymakers should consider the status of medical datasets where key identifiers are removed in greater granularity.
- Issuing clear guidance on the legal bases for processing and transparency under the GDPR, including outlining how various GDPR legal bases for processing align with use cases that are fundamental to the development of data-driven innovation in the life sciences. Key areas of the product lifecycle, such as post-market surveillance, clinical follow-up and scientific research should be mapped against the various legal bases described in both Articles 6 and 9 of the GDPR.

SERVICE DELIVERY

The performance of DHTs can often be impacted by the service in which they are utilised and certainly, in the case of machine learning, the data flows they are exposed to. To ensure safety it is vital that we have an understanding of the data flows into the DHT and the output provided. This data needs to be made available to the DHT provider, in a suitable anonymised format, as a matter of course.

It is also critical that there is responsibility and control of the data flows into DHTs that are controlled by the health system and within the healthcare settings.

Particularly for AI, tools and best practice are needed to demonstrate trustworthiness on how:

- The DHT is behaving as predicted.
- Output is changing during clinical use.
- Software can be rolled back to previous states, or rolled forward to a safe state.
- Bias could be introduced, detected and rectified in the system.
- Processes are in place to evaluate and characterise data for AI.

A standardised approach to Data Protection Impact Assessments would support this.

IMPLEMENTATION

There are important considerations outside of regulation and standards that can have a significant impact on the performance of the system. We would recommend that the following areas are explored jointly with industry to ensure the system is implemented in a manner that reduces bureaucracy and streamlines processes. This will support faster patient access and position the UK as an attractive investment and launch market:

- Greater use of/access to regulatory sandboxes.
- Single audit and digital audit processes.
- Education and advice services.
- Published timelines and stage gate criteria.
- Regulators should consider risk-based mechanisms that enable pre-qualification of algorithms, platforms or companies to speed up regulatory approvals.
- Robust working processes between regulator and conformity assessment bodies.
- Strong alignment between MHRA policy and enforcement teams and with Conformity Assessment Bodies.

International Alignment

- To support UK developers, we need a global approach to regulation rather than focus on EU mutual recognition, the latter being unlikely in near term.
- There is a possibility to work on underpinning technical requirements.
- Will need to demonstrate trustworthiness of a UK regulatory system to work towards longer term trading arrangements.
- Utilise IMDRF to drive international recognition of UK processes and classifications.
- Global alignment on data privacy would be ideal, currently need to deal with national or state legislations.

NEXT STEPS

There are a number of broad areas that require further investigation and cross organisational collaboration. A group should be established of key regulators, health system leaders and industry to develop proposals relating to:

1. Scope: Demarcation between medical device and health & well-being applications is unclear and can be altered based on how products are marketed and their related claims. There needs to be a clear scope for what is in the regulatory regime based on risk and pragmatic assessment of system capability and capacity.
2. Transparency: Guidance from relevant agencies on qualification process for apps/AI, with use of standards in applications where more certainty is required.
3. Classification: Global regulatory frameworks for medical technologies tend to follow a risk-based approach, however the specific classifications/tiers/grouping vary. We need to assess what is an appropriate classification regime for UK Digital Health regulation based on scope above, international alignment, existing UK frameworks (e.g. UKCA, NICE, ESFs etc.) and building public and system trust.
4. Post Market Surveillance: The necessary infrastructure and processes need to be established to enable the use of real world and real-time data from DHTs to deliver a more responsive, scalable and agile PMS process. Current reporting mechanisms may not be operationally practical to scale up when applied to DHTs.
5. Artificial Intelligence: There are specific issues with the regulation of AI due to its inherent functioning. These need addressing building on existing work both in the UK and internationally, in a manner that is both rigorous and supportive of the UK becoming a destination for AI health innovators.

REFERENCES

1. https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health Accessed 28/04/2021

2. MHRA Guidance: Medical device stand-alone software including apps (including IVDMDs) v1.06

3. New legislative framework: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en Accessed 28/04/2021

4. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550542/Prof_Christopher_Hodg es_ -_Ethics_for_regulators.pdf Accessed 15/11/19

5. https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program#program Accessed 15/11/19

6. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf Accessed 28/04/2021

7. A guide to good practice for digital and data-driven health technologies - GOV.UK (www.gov.uk) Accessed 28/04/21

8. https://insightplus.bakermckenzie.com/bm/healthcare-life-sciences/united-kingdom-an-open-letter-to-policymakers-we-need-to-talk-about-the-real-issue-with-health-data-regulation Accessed 28/04/21

9. https://www.hsj.co.uk/technology-and-innovation/nhs-staff-tremendously-anxious-over-data-sharing-says-new-national-leader/7029975.article Accessed 28/04/21

GLOSSARY

AI: Artificial Intelligence

CQC: Care Quality Commission

DHTs: Digital Health Technologies

DTAC: Digital Technology Assessment Criteria

ESFs: European System of Financial Supervision

GDPR: General Data Protection Regulations

ICO: Information Commissioners Office

IEC: International Electrotechnical Commission

IMDRF: International Medical Device Regulators Forum

ISO: International Organization for Standardization

IT: information technology

mHealth: mobile health

MHRA: Medicines & Healthcare products Regulatory Agency

NICE: National Institute for Health and Care Excellence

NIS Regulation: The Security of Network & Information Systems Regulations (2018)

PMCF : Post-Market Clinical Follow-up

PMS: Post Market Surveillance

QMS: Quality Management System

SaMD: Software as a Medical Device

UKCA: United Kingdom Conformity Assessment

June 2021

Association of British HealthTech Industries
Suite 2, 4th Floor, 1 Duchess St,
London, W1W 6AN

+44 (0)20 7960 4360
enquiries@abhi.org.uk
www.abhi.org.uk
@UK_ABHI