UKAuthority Inform

geoplace®

April 2023

Sharing data to support vulnerable people

Requirements for standardisation, attribute flags, location data and information governance in the identification and support of vulnerable people

Key steps summary

- Identify vulnerability risk attributes and the datasets where they reside.
- Identify partners for data sharing.
- Consider the information governance aspects.
- Use the SAVVI catalogue on data sharing propositions.
- Use UPRNs as the key to linking datasets. This minimises the use of personal data while maximising the benefits of sharing

Now read on...

"Given that 100s of local authorities are all often trying to achieve the same thing, would it not be more efficient and effective to take a centralised approval approach to a shared problem?"
Service Manager, a City Council

Contents

1. Ambition built on evidence

As Covid-19 swept the country early in 2020 there was an urgent need to rapidly share data across health and local public services. In an unprecedented move the Secretary of State for Health and Social Care issued a Control of Patient Information (COPI) Notice[1] requiring the NHS to share appropriate confidential patient information with organisations in the local authority sector that it deemed entitled to process this for Covid-19 purposes. This notice expired on 30 June 2022.

But it has left a lasting legacy; having demonstrated the immense value of sharing up-to-date, relevant information to identify and support vulnerable people, the experience has driven an ambition among local health and public service providers to 'do more with data'.

A key learning from Covid was the value of minimising the sharing of data while maximising its appropriate use and value through sharing 'flags' linked to properties, rather than individuals. This also highlighted the value of data standards as a key to link and explore data, with the unique property reference numbers (UPRNs) within core councils and Ordnance Survey datasets playing a significant role.

Since then, a more ambitious way of thinking about sharing data to identify and protect vulnerable people has emerged in the public sector as we move from one crisis to the next, in the shape of the cost of living and fuel poverty.

There is a strong desire to make further progress, but also an acknowledgement of technical and legal barriers to be overcome, and a sense that the understanding of how to make it work is incomplete. Organisations are still working on ways to share vulnerability data effectively and within the relevant legislation.

UKAuthority, in partnership with GeoPlace, explored this key issue through a series of UKA Live discussions with public sector experts including the Information Commissioner, Central Digital & Data Office, Barnsley Council, NHS England, Humberside FRS and iStand/SAVVI, and reviewed relevant initiatives. This paper is aimed at strengthening common understanding of how to approach the task, with an investigation of the key factors, details of the main sources of guidance and examples.

2. The core challenge – the need to standardise

Although the pandemic has subsided, the rationale for sharing vulnerability data remains strong. There is a consensus that it can strengthen the day-to-day provision of relevant services, helping to ensure they are directed at the right individuals and groups in a community, and help to prepare organisations for dealing with any future crises. It is not just about identifying the people in need but understanding the factors that lead to vulnerability and how to plan services in response.

There are plenty of examples of best practice – the research has highlighted efforts by Barnsley Council, the Welsh Government and Humberside Fire and Rescue Service – but the overall picture is fragmented. There is no widely held consensus on how to approach the task and many public authorities are still held back by fears of breaking data protection laws. Complex issues have to be addressed before a more cohesive outlook emerges.

This relates in part to a need for greater standardisation around the data and definitions of vulnerability risk. It was brought up in the discussions that different organisations can have their own versions, influenced by the nature of their services, of what is meant by vulnerability and how it should be applied.

> *"I work across the ICS. We have the working relationships, willingness to share data and work together but knowing what indicators to combine to identify vulnerabilities would be so helpful."*
> **Public Health Intelligence Specialist, a City Council**

This makes it harder to identify the key datasets and datapoints in any collaboration, leading teams to query why others want access to a specific piece of data, and complicates finding common ground to justify sharing.

> *"The NHS shared data on the clinically extremely vulnerable to provide focus for a place based response. This access was then withdrawn yet we now face another health crisis through cost of living. NHS colleagues understand the need for vulnerable data yet the system as a whole appears reluctant to share again."*
> **Head of Corporate Services, a District Council**

It applies down to a granular level. There is currently no agreed list of shared indicators for different types of vulnerability or a formal process for how they should be used, which makes it more difficult to co-ordinate work in protecting vulnerable people. Among the comments in the discussions was: "One of blockers is there is no common opinion on which piece of data is a good predictor of a particular vulnerability. What are the key predictor attributes we need to unblock and get access to?"

Some organisations see indicators for vulnerability in factors affecting individuals such as employment status, physical mobility and receipt of specific benefit payments, but this can be subjective and open to disagreements. Similarly, the use of demographic data at a geographic or community level is subject to differing judgements on its value that may get in the way of it being shared.

Another challenge needing a more standardised approach is the data sharing agreements between organisations. The point made in discussions was that these are currently fragmented, with organisations having to set up their own agreements, often for a specific purpose and with multiple clauses tying it to this purpose alone.

Indeed, for any agreement there must be a sound reason for using the data, related to a specific vulnerability, and with a particular outcome. This can force organisations to feel they have to start afresh for any new data sharing arrangement – which is time consuming and sets up another barrier to overcome. There is a clear need for a more standardised approach through use of templates and shared examples of best practice, with the scope to add clauses for specific instances, to reduce the burden and get arrangements in place more quickly.

Overall, the public sector is still trying to find common markers, although some organisations have made notable contributions. Barnsley Council has created a

vulnerability index (outlined in the case study box) that helps to support vulnerable people but shields their identities from anyone who does not deal with them directly.

A SAVVI approach

More widely, development of the SAVVI[2] (Standard Approach to Vulnerability via Interoperability) standards is a key step in development of a common process. It is part of the iStandUK[3] programme to promote data standards – led by Tameside Council and supported by the Department of Levelling Up, Housing and Communities – and aimed at providing a more consistent view of vulnerable people and households, and building confidence in sharing data on a range of vulnerabilities.

It has developed a set of standards for its consent model, logical model, recommended messaging formats and data structures, and identified a set of data attribute flags as indicators of vulnerability (see box). These can be used to predict needs and later provide evidence of outcomes from an intervention.

The SAVVI team is building a catalogue of the attributes, urging technology suppliers to provide solutions that can incorporate them, working on common approaches to sharing the data, and plans to republish its declaration[4] on tackling vulnerability through improvements in data sharing. It also has a longer term ambition is to build a trust framework in which data can be shared 'as a service', with confidence that only the minimum information is passed to those with a right to receive it.

It also provides guidance on the roles that different organisations can play when a multi-agency response is needed.

Data Attribute Flags as Indicators

Source: SAVVI

Potential Homelessness...

- UC benefit cap / rent gap
- Offending / anti-social behaviour
- Domestic violence
- Police called to domestic incident
- Mental health problems
- Drug or alcohol incident / support

Loneliness / Financial Distress...

- Living alone
- In arrears
- Moved home
- Recently bereaved
- Lost job
- Over 70

School Readiness...

- Maternal education
- Household income band
- Household number of children
- Gender

New Need for Care...

- GP registrations - and who is not registered
- Multiple GP appointments
- Multiple A&E attendance
- Multiple 999 calls

"The Unique Property Reference Number – the unique identifier for every addressable location – is key to almost everything that's delivered or achieved by councils."
Local Government Association guidance for councils

Barnsley's vulnerability index

Prompted by the pandemic, Barnsley Council created a vulnerability index[32] with an assigned risk score against individual residents. This took in 26 data sources, internal and external, with a series of weighted flags to emphasise their relative importance, and automation to ensure capability to call off information as required. Personally identifiable information is standardised and written to a master file in the council's data warehouse, ensuring that field names, formatting and syntax is consistent.

A key feature is the use of unique property reference numbers (UPRNs) with a data linking and matching process to ensure it is in place for any households where the source information did not store it. This ensures a system-wide mechanism for checking data integrity and preventing duplicate entries, and makes it possible to identify issues by household rather than individual.

Analysing by address will also show whether there is anyone else in the household that has interactions with the council. Any personal data is only made available when council officials see the need for an intervention and to make contact with the household.

The index was used to contact 14,000 households during the pandemic with advice on issues such as shielding and applying for food deliveries. It has also been applied to functions such as identifying people with council tax arrears who have genuine problems affecting their ability to pay, and the council's Supporting Families programme, supporting internal collaborations and interventions.

Currently a library of indicators enables work with internal teams requesting information to identify appropriate indicators for a particular programme. Moving forward, Barnsley is working with key partners in social housing, police and the NHS in a Barnsley Data Group to explore the benefits and practicalities of sharing vulnerability data more widely.

"We are matching: People over 70, Assisted Bin Lifts, Vulnerable Tenants, Food Bank requests, CAB enquiries."
Example from a District Council, UKA Live Attendee

3. UPRN - the key

Created by local authorities and managed nationally by GeoPlace[5], UPRNs provide a unique numerical identifier for each and every addressable location in the UK.

They are used by local authorities, mandated for use by central government[6], and advised for use by the Local Government Association[6.1] (also included in its Local Government Digitalisation Almanac)[6.2] as the open standard to follow. Guidance from the Central Digital and Data Office in August 2022[6] states that UPRNs and the associated unique street reference numbers (USRNs) enable the public sector to:

- accurately identify property and street location information;
- link information in different datasets;
- share consistent data and reduce errors when exchanging location information between systems;
- link to definitive address and street information contained in Ordnance Survey products.[7]

In public services 'everything happens somewhere'. Incorporating UPRNs in datasets makes it possible to combine risk flags as alerts of potential problems at household rather than the individual level, with relevant attributes then shared only with those in appropriate roles – which helps to maintain confidentiality. This focus on a property rather than an individual can help ensure sharing remains within the terms of the Data Protection Act 2018[8].

Their value is widely recognised by local authorities and they are consistently used internally. But discussions acknowledged

"UPRNs are a core part of our data and digital infrastructure, we need to get more people understanding the benefits of open standards and open identifiers for data linkages. In policy terms, UPRNs are really important for improving policy and citizen outcomes and understanding market efficiency across housing, planning and other DLUHC policy areas."
Lawrence Hopper, Deputy Director for Digital Policy at DLUHC

Humberside's fire fatality risk index

Humberside Fire and Rescue Service (FRS) has developed a fire fatality risk index to identify vulnerable people and vulnerable property.

This has been greatly assisted by a data sharing initiative between the National Fire Chiefs Council (NFCC) and NHS England resulting in the Exeter Data, which identifies people over the age of 65 in order to offer home safety checks. These checks provide advice on fire safety within the home, which is leading to a reduction in domestic fire related deaths and injuries – over 50% of such fires occur in households where over 65-year-olds reside.

Head of risk and intelligence at the FRS, Jo Mann, has added a frailty score to the Exeter data along with information on mobility and shopping (smoking) habits from Experian's MOSAIC data. Other common vulnerability factors that Mann says linked to fire risk include:

- history of falls;
- smoking;
- alcohol use;
- frailty;
- mobility issues;
- single household;
- assisted bin collection;
- rented accommodation.

Mann has been clear on the difficulties of combining such a wide variety of information when the UPRN is not used – during Covid this significantly slowed analysis work for the local resilience forum. Having UPRNs within core datasets means that fire services can rapidly share citizen-centric information to provide household-level support.

Indeed, a 2017 report for the NFCC reviewing its use of big data[9] , noted that preparation and cleansing of large datasets to remove or correct anomalies, and miscoding and to prepare the data for linkage or layering represents a major, time consuming task in most cases. It highlighted that for the Exeter Data the lack of a UPRN was a significant issue.

that UPRNs are still not used by all externally and by many other public sector bodies - and some of those that do are not systematically adding them to ALL relevant datasets, which makes it harder to break down the barriers in sharing vulnerability data.

There was a push to attach these unique identifiers more widely during the pandemic, but anecdotal evidence suggests that without an immediate crisis this momentum risks being lost.

> ***"In the pandemic we saw that just one organisation (ie the NHS or DWP) not being aware of the importance of the UPRN for joining data together can massively hinder productivity and decision making. How can we challenge these bodies effectively?"***
> **Anonymous UKA Live attendee**

Officials familiar with the immense value of UPRNs as an open identifier for data linkage agree that this needs to be corrected as it is significantly harder to identify vulnerable people when they are not used - plus there is a danger of undermining any response to the next crisis. To help build confidence within organisations about their use, GeoPlace has collated excellent guidance and a wealth of case studies[8.1] that councils and others can draw on.

As the UPRN is connected to property and people often move home there is of course a need to ensure that any flags indicating vulnerability are reviewed in real time and that there are robust processes in place – potentially supported by automation – to ensure that flags are kept up to date.

4. Information governance

"In my council, we want to share but do fear the penalties if we get this wrong..."
Anonymous UKA Live Attendee

A significant barrier to data sharing remains in the pervasive uncertainty over the complexities in data protection laws and the correct approach to information governance (IG).

Legislation is dry, complex and complicated - sometimes seemingly contradictory and open to interpretation via case law. To complicate matters further, lawyers in different public sector organisations can hold different opinions and interpretations of best practice.

Many organisations were constrained by a fear of breaking the law before the pandemic, then became more confident in doing so, due to the sense of urgency and the direct provisions brought in with the COPI notices. With expiration of the notices uncertainty re-emerged, despite indications in the data strategy for health and social care[10] – published in June 2022 – that the Government plans to amend them "to facilitate timely and proportionate sharing of data".

There is still a sense of uncertainty and fear of breaching the Common Law Duty of Confidentiality in relation to health data that acts as a barrier.

Meanwhile the Cabinet Office published its Data Sharing Governance Framework[11] in May 2022, which includes a section on a responsible approach to the process. But this deals with generalities, citing steps such as getting assistance from data protection professionals, making it easy for users who want to access data to identify the relevant laws, and collaboration on data protection impact assessments (DPIAs). It does not deal with the guidelines for specific types of data or use cases such as supporting vulnerable people.

"GDPR says no is probably the most common thing I hear when talking to people about data sharing for any purpose."
Anonymous UKA Live attendee

The UK's implementation of the General Data Protection Regulation (GDPR) - laid out in the Data Protection Act 2018[12] - balances the rights of individuals with the responsibilities of organisations to process data for the public good. This means that any initiatives, even when supporting vulnerable people, have to be balanced in terms of proportionality and purpose, which often requires a risk based approach to sharing data.

"The Digital Economy Act allows data to be shared in order to identify and support those living in fuel or water poverty - including doing things like actions to improve their economic wellbeing."
Head of Data Ethics and Data Sharing, UKA Live Attendee

There is scope for a more open approach within the Digital Economy Act 2017[13], which includes legal gateways for sharing some personal data to improve public service delivery on condition that the objective is to improve the wellbeing of individuals or households, including their physical and mental health, social and economic wellbeing.

However, this must be balanced with the confines of the Data Protection Act and, in the case of health information, the Common Law Duty of Confidentiality[14].

Meanwhile, a new Data Protection and Digital Information Bill[15] was presented to Parliament in July 2022, then revised and resubmitted in March 2023, seeking to replace the GDPR privacy system with an updated, simplified UK data protection framework post-Brexit. Of particular pertinence to this paper, the new bill contains specific provisions about the disclosure of information to improve public service delivery – and the safeguarding of vulnerable individuals.

In light of the complexities of information governance it is no wonder that many lack confidence in their ability to share information. However, there is much cause for optimism in an ongoing sea-change sector-wide from a focus on 'what should not be done' to an emphasis on 'what can be done'.

The Information Commissioner's Office[16] has a definitive guide to the UK General Data Protection Regulation (UK GDPR)[17] and has issued a useful data sharing code of practice that covers almost all data sharing scenarios[18] , plus a guide to the Digital Economy act codes in data sharing across the public sector.[19]

5. Culture and skills

Discussions highlighted that standards and legislation are not the only barriers to data sharing across government - cultural and organisational barriers can be even more of a problem, including a general lack of awareness of powers, fears about using them and different levels of capability and capacity across the sector.

Changing the emphasis from a default 'computer says no' approach to 'how do we do this' not only requires a general culture shift but also investment in skills, capacity and interoperable infrastructure.

Government has ambitions to create a joined up and interoperable data ecosystem for the public sector across the whole of the UK, whilst ensuring high levels of public trust.

To successfully deliver this there must be investment and a shift in focus to the benefits of sharing data, the missed opportunities and the potential harms of not sharing information. There must also be an open approach to 'what next', war gaming potential scenarios and crises that will require a rapid response to data sharing – what might be the next Covid, cost of living or other crisis that the public sector will need to respond to in protecting and supporting citizens?

Engaging the public from the start about how their data is currently used is critically important, as is the need to drive data literacy around how data sharing will help them – many see no issue with sharing details of their lives across social media, but worry that 'Big Brother' is watching. Building trust in how the public sector uses data is essential to gaining public support for the effort.

This does not mean that everyone – citizens and the public sector – must become experts in data law. Indeed, the discussions emphasised the need for targeting and communicating different levels of understanding to different groups. The public, for example, only need to feel right about how their data is being used; frontline staff do not need to know the intricacies of information governance (IG) but do need clarity on what they can do; whereas IG professionals need to know what the laws say and how to apply them. They must be clear about what their organisations are doing and the obligations involved, relating this to purpose and proportionality.

JIGSO in Wales

The Welsh Government has identified the protection of vulnerable people as one of its data priorities, prompted by the experience of the pandemic and more recent crises emerging from the rise in the cost of living and energy prices. It has wanted to do as much as it can over the winter of 2022-23 and build its data readiness for the longer term challenge.

Its Joint Emergency Services Group (JESG) has previously worked with GeoPlace, Ordnance Survey, and Welsh local authorities on a pilot scheme known as JIGSO ('jigsaw', in Welsh) – using UPRNS to collate information about individuals' vulnerability on an address-by-address basis.

This used the identifiers in linking data from adult social services departments in the Mid and West Wales and local emergency services teams to provide a picture of households more likely to be at risk. An early benefit was in enabling the region's fire and rescue service to carry out more effective fire safety checks on the homes of vulnerable people. A second phase led to the Dyfed Powys resilience team identifying all the vulnerable properties in the area ahead of any potential major incidents.

The data is shared through a secure platform – currently manually but with plans for it to be automated – and draws on APIs from the various sources.

In essence, JIGSO enables Wales's core non-personalised datasets to be made available to the resilience community, as a free to use service. It makes it possible to identify 'at risk' households and supports collaborative planning between local agencies such as emergency services, hospitals and care homes. It is not a new system or piece of technology, but a process that optimises UPRNs, and hinges on the 'create once, use many times' principle to reduce the time it takes to get key information to responders.

The main users of JIGSO have been local authorities and emergency services, often through local resilience forums. Such an approach can also work for other services, such as utility providers that have a statutory duty of care towards people who may find it harder to access of pay for their services, or need them to ensure their health and wellbeing.

6. Guidance and further information

While there are open questions and grey areas that complicate the issues, as outlined above there are key documents that set out the legal boundaries of sharing data and the approaches recommended by central organisations.

The Data Protection Act, incorporating the General Data Protection Regulation[20], outlines the latter along with the requirements for general processing, law enforcement processing, rights of the data subject, the roles of controller and processor, functions of the ICO and other issues.

The Digital Economy Act[21] includes a section on digital government that provides legal gateways for specified public authorities to share data with each other, some of which cover the sharing of personal data while others are relevant to non-identifying data.

The Government Data Sharing Governance Framework[22] – aimed at senior leaders, data management specialists, data practitioners and requesters – says that sharing should be a strategic priority but emphasises it should be done in a responsible manner. This includes getting assistance from data protection professionals when considering an initiative, making it easy for users to identify the laws that make it possible, making it easy to collaborate on DPIAs, ensuring that users can access information on existing DPIAs and agreements, and making sure users can easily access non-sensitive or non-personal data.

The ICO Data Sharing Code of Practice[23] highlights key principles of the UK GDPR, good practice in data sharing agreements[24] and the lawful basis for sharing data[25]. It also provides a guide to the Digital Economy Act Codes[26], saying they do not currently cover the provision of health and social care, but that there is one "to assist people experiencing multiple social or economic disadvantages, or living in fuel or water poverty".

SAVVI[27] is essentially a work in progress, but it is being actively used and comes with a process for identifying then mobilising support[28] for vulnerable people in a community. It does not set out prescriptive steps or actions, but emphasises that a well defined purpose and end-to-end process should accelerate data sharing. It also includes data standard definitions[29] that could be of value to local authorities and their partners.

> ***"We have a data sharing code of practice that covers almost all of the data sharing scenarios; also a guide on how GDPR relates to DEA 2017."***
> **Dr Susheel Varma, ICO**

GeoPlace has rounded up the guidance on using UPRNs[30] and unique street reference numbers (USRNs), and undertaken a research project with the LGA on the role of UPRNs in delivering health and social care[31.1] and their use in supporting vulnerable people[31.2].

7. The key steps in full

Unquestionably, data sharing is key to unlocking improved public services – to identifying and supporting vulnerable people.

The public sector is finding its way in sharing vulnerability data, and the dynamics are likely to vary for each organisation and the community they are aiming to protect. But there are a number of key steps that will be relevant to most initiatives and long term efforts to refine and make the practice more effective. The basics are as follows:

- **Start with the goal of minimising the sharing of personal data** - focus on property and essential anonymised attributes to achieve the purpose.
- **Identify vulnerability risk attributes** that are likely to indicate a particular vulnerability and the datasets where they can be found. These will vary between organisations and different types of vulnerability, but there is a growing understanding of which ones are crucial, and increasing opportunities to learn from the experience of other authorities.
- **Identify partners** – the organisations holding data that are likely to make the efforts more effective – and open the dialogue for sharing.
- **Consider IG** from the outset and how the prospects relate to the Data Protection Act, Digital Economy Act and ICO codes of practice and use these to establish data sharing agreements.
- **Be SAVVI** - When it becomes available, be ready to consult the SAVVI catalogue on data sharing propositions.
- **UPRNs are the key** – Harness the power of UPRNs, ensure they are attached to datasets and be ready to use them as the key to linking information. This will help to identify potentially vulnerable households rather than just individuals.

These can facilitate the immediate efforts, but more can be done to build a long term capability:

- Encourage the attachment of UPRNs to any datasets for which they are relevant, both internally and among partners.
- Develop a process for the removal of a UPRN-linked flag from a dataset specific to vulnerability once the relevant individual is no longer at risk, or has moved to another address or is deceased. Investigate the potential for automating this process.
- Be ready to collaborate with organisations looking to standardise their data to common practice.

The last of these is one that needs widespread collaboration, preferably within a formal programme such as SAVVI, and will be crucial to providing a strong foundation on which data sharing can evolve.

As more organisations see the value of sharing this data, they will need a clear understanding of how it should be structured, the requirements for interoperability and the most important attributes. This will include many smaller organisations – down to the level of domiciliary care providers and individual care homes – without much data capability and who need clear leadership. But all those with the resource to continually look for improvements in their data can make a contribution.

With an impending new data bill the landscape will inevitably change over time, and there will be scope to develop new initiatives in data sharing for the common good. These could become more complex, taking in new factors and harnessing the potential of machine learning and artificial intelligence.

But the underlying principles of finding the attributes that can indicate vulnerability and using them proportionately within the legislation will remain as the foundations for the long term.

This will be important to the public sector as, with rising demands on its services and the squeeze on its finances, it needs to place a greater emphasis on preventative rather than reactionary measures. Much of its resource goes into supporting people who are vulnerable, and the earlier it can take action the lower the overall burden will be to both individuals and the organisation.

8. The discussions

As a core part of the research for this briefing note, UKAuthority's publisher, Helen Olsen Bedford, hosted two UKA Live discussions exploring emerging best practice on the local public services front line and the legal frameworks within which local service providers must operate as they seek to identify and support vulnerable people durig the current cost of living crisis. Both discussions can be viewed in full at www.ukauthority.com.

UKA Live: Harnessing data to support the vulnerable

How can we build on the data sharing experience gained during Covid to meet the current challenges facing our communities?

Jamie Tasker, BI Innovation Manager, Barnsley Council

Jo Mann, Head of Risk & Intelligence, Humberside Fire & Rescue Service

Paul Davidson, CDO, Sedgemoor District Council / Director iStandUK and SAVVI

Richard Duffield, Head of Customer Insights, GeoPlace LLP

Watch now

UKA Live: Data, IG and supporting the vulnerable

What are the legal rights – and duties – to share data to support vulnerable people?

Dawn Monaghan, Interim Director of IG Policy, Ethics and Head of Profession, NHS England

Dr Susheel Varma, Head of AI & Data Science, ICO

Murat Soncul, Head of Privacy and Data Protection, Central Digital and Data Office

Richard Duffield, Head of Customer Insights, GeoPlace LLP

Watch now

GeoPlace LLP is the central source of information for all UK addresses and streets. It manages the data that officially defines more than 46.5 million addresses and 1.58 million streets in the UK.

It is the guardian of the UK's Unique Property Reference Numbers (UPRNs) and Unique Street Reference Numbers (USRNs), responsible for collating, managing and maintaining the primary UK authoritative geospatial address and street datasets.

GeoPlace LLP was created when the then Secretary of State for Communities and Local Government called for a standard index of addresses to be created, to help the UK work more efficiently. A joint venture was set up between the Local Government Association and Ordnance Survey to build the National Address Gazetteer infrastructure and National Street Gazetteer. OS develops the range of AddressBase products from the National Address Gazetteer and OS MasterMap Highways Network from the NSG.

Bringing location to life with the power of data.
Find out more at **www.geoplace.co.uk**

UKAuthority

This briefing note has been researched, written and published by **Mark Say** managing editor & **Helen Olsen Bedford** publisher, UKAuthority.

UKAuthority champions the use of fire, health and housing, to improve services for the citizens they serve.

Image sources: iStock-iLexx | iStock-metamorworks

References

[1] https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/control-of-patient-information-copi-notice | [2] https://coda.io/@savvi/welcome/the-process-5 | [3] https://istanduk.org/ | [4] https://coda.io/@savvi/welcome/the-savvi-declaration-167 | [5] https://www.geoplace.co.uk/addresses-streets/location-data/the-uprn | [6] https://www.gov.uk/government/publications/open-standards-for-government/identifying-property-and-street-information | [6.1] https://www.local.gov.uk/our-support/research-and-data/data-and-transparency/using-unique-property-reference-number-uprn | [6.2] https://www.local.gov.uk/our-support/cyber-digital-and-technology/almanac | [7] https://beta.ordnancesurvey.co.uk/products/addressbase-premium | [8] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [8.1] https://www.geoplace.co.uk/local-authority-resources/guidance-for-custodians/case-studies | [9] https://www.nationalfirechiefs.org.uk/write/MediaUploads/NFCC%20Guidance%20publications/Sector%20improvement/CFOA-Big_Data_Report_2017.pdf | [10] https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data/data-saves-lives-reshaping-health-and-social-care-with-data | [11] https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework | [12] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted | [13] https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted | [14] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care/hscic-guide-to-confidentiality-references | [15] https://bills.parliament.uk/bills/3322 | [16] https://ico.org.uk/ | [7] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ | [18] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/ | [19] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-across-the-public-sector-the-digital-economy-act-codes/ | [20] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted | [21] https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted | [22] https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework | [23] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/ | [24] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/ | [25] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/lawful-basis-for-sharing-personal-data/ | [26] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-across-the-public-sector-the-digital-economy-act-codes/ | [27] https://coda.io/@savvi/welcome | [28] https://coda.io/@savvi/welcome/the-process-5 | [29] https://coda.io/@savvi/welcome/standards-14 | [30] https://www.geoplace.co.uk/addresses-streets/data-in-use/guidance | [31.1] https://www.geoplace.co.uk/addresses-streets/data-in-use/uprns-delivering-health-and-social-care | [31.2] https://www.geoplace.co.uk/blog/2022/we-can-support-the-vulnerable-more-effectively-when-we-know-where-they-are | [32] https://www.geoplace.co.uk/case-studies/barnsley-council-using-the-uprn-to-build-a-vulnerability-index