Schedule 8

Data Sharing Agreement

Agreement between the Authority and the Contractor

1. In order to carry out TB testing services, Contractors need to have access to data stored on DAERA’s computer system, currently the Northern Ireland Food and Animal Information System (NIFAIS). The data being shared between the Authority and the Contractor are herd and Keeper data.
2. Data from NIFAIS will be downloaded onto the Contractor’s IT equipment, PCs, laptops and handheld devices for use on farm. There is a risk that herd and Keeper data could be accessed by individuals who are not involved in TB testing. Such unauthorised access could result in misuse of the data.
3. In order for data security to be maintained, good data handling practices must be in place and Contractors must be responsible for the security of data which has been downloaded from NIFAIS.
4. A Data Sharing Agreement (DSA) which specifies the Contractor’s required data handling practices and responsibilities to keep data secure must be signed. The DSA governs the transfer or sharing of information from the Authority with the Contractor for the purpose of carrying out TB testing services.



DATA SHARING AGREEMENT BETWEEN

Department of Agriculture and

Rural Development (DAERA)

Veterinary Service (the Authority)

and

the Contractor

Data required for Bovine TB testing services

|  |  |  |
| --- | --- | --- |
| 1. | **Parties to the agreement** | |
| **The Authority:**  DAERA  Jubilee House,  111 Ballykelly Rd,  Limavady,  Co. Londonderry,  BT49 9 HP  Data Protection no.- Z6402243 | **The Contractor:**  [Practice Name]  [Address]  Data Protection no. - [ ] |
| 2. | **Introduction**    The Authority requires the Contractor to carry out TB testing services.  In order to carry out these services, the Contractor will use e-PVP to either print off test sheets or download information from NIFAIS to their IT equipment, Personal Computers or Laptops. Downloaded information can then be transferred electronically onto handheld devices  This information facilitates the Contractor in carrying out the TB test.  Following testing, e-PVP is again used by the Contractor to   * Input written results manually onto NIFAIS from details recorded on the test sheets * Transfer test results from the handheld device on to the Contractor’s IT equipment and then upload to NIFAIS | |
| 3. | **Purpose**  **This document is an agreement which governs the transfer or sharing of information from the Authority with the Contractor (contracted veterinary practice) for the purpose of carrying out TB testing.** | |
| 4. | **Legal Basis for Data Sharing**  Sharing of this Data is necessary under the following legislation:  The Diseases of Animals (NI) Order 1981(as amended);  Tuberculosis Control Order (NI)1999 No 263  Sharing of this Data is lawful under the following legislation:  Data Protection Act Schedule 2 Condition 6 – Processing necessary for the purposes of legitimate interests pursued by the data controller. | |
| 5. | **Data to be Shared**  Information held on NIFAIS to enable the Contractor to carry out testing services, includes personal information such as names, addresses and herd details. | |
| 6. | **Information use**   * The Contractor will **only** have access to NIFAIS to enable them to carry out testing services as detailed in this contract. * The Authority will remain the Data Controller at all times. * The Contractor must not share this information with any Third Party. * In the event of the termination of the contract the Contractor’s access to NIFAIS for TB testing services will be terminated. | |
| 7. | **Requests for information**  If the Contractor receives a request for information relating to the Authority’s data as covered by this agreement, it will be the responsibility of the Contractor to contact the Authority as set out below, who will determine the handling of the information and respond to such requests:  Data Protection Act, Freedom of Information or Environmental Information Regulations  DAERA VS  Information & Communication Branch,  Room 733,  Dundonald House,  Upper Newtownards Road,  Belfast  BT4 3SB  Tel: 028 90524716  Email: [vsinfo&commsbranch@daera-ni.gov.uk](mailto:vsinfo&commsbranch@daera-ni.gov.uk)  The Contractor must assist and co-operate with the Authority to enable them to comply with all information disclosure requirements. | |
| 8. | **Responsibilities of each party**   * The Authority remains the Data Controller at all times. * The Contractors access to NIFAIS is for the sole purpose as described in these contract documents * The Contractor must ensure that adequate steps are taken to prevent –  1. Accidental or deliberate destruction of the information; 2. Accidental or deliberate modification of the information; 3. Unauthorised access to information or to any computer system or mobile device containing the information; 4. Misuse of the information; 5. Loss of data (refer to section 11).  * The Authority can at any time request access to printed documentation to ensure that security protocols are in place for security audit purposes. The Authority also reserves the right to seek assurance that the correct disposal of paper documentation has been carried out at the end of the Contract. * The Contractor must ensure that all the Authority’s data held on handheld devices is encrypted. * The Authority will ensure that all information/data downloaded from NIFAIS by the Contractor is encrypted at source. * The Authority reserves the right to suspend or terminate the Contract if this Data Sharing Agreement is not complied with. | |
| 9. | **Security**  All information must be handled in accordance with Government guidelines for handling and processing personal information and the Contractor must comply with the Data Protection Act 1998 and must adhere to DAERA’s Information Security Policy Section 5 – Mobile Device Security as it relates to contractors.  The contents of document DAERA’s Information Security Policy Section 5 – Mobile Device Security is reproduced at the end of this section.  **The seventh principle of the Data Protection Act states that “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.”**  The Contractor and their staff, who process data on behalf of the Authority, must be fully aware of, and abide by, their duties and responsibilities and comply with the eight principles of the Data Protection Act 1998.  **Personal data shall be:**   1. Processed fairly and lawfully; 2. Processed for limited purposes and in an appropriate way; 3. Relevant and sufficient for the purpose; 4. Accurate; 5. Kept for as long as is necessary and no longer; 6. Processed in line with individuals’ rights; 7. Secure 8. Only transferred to other countries that have suitable data protection controls.  * Personal/restricted data that is stored/located in private premises or removed from these premises to be utilised in the field for business purposes must be processed in line with above mentioned Act. * Data extracted from NIFAIS must be processed for the purpose of this agreement only. This data should not be released to a Third Party without the prior knowledge and explicit consent of the Authority. Any misuse of this information will result in a breach of the agreement. * Any paper copies printed must be securely stored in locked cabinets which are only accessible by authorised staff. * The Contractor and their staff are required to keep Personal Digital Assistants (PDAs) and paper documentation with them at all times when travelling, and ensure that they are never left unattended when outside their business premises. * The Contractor must ensure PDAs and paper documentation, kept on their business premises, are securely stored in a lockable cupboard or drawer and are protected from unauthorised use or access by another person, and from accidental corruption caused, for example, by spillage or breakage. * When utilising e-PVP all ID codes and passwords must be stored securely and changed on a regular basis. * The Authority advise that in order to achieve best practice a Tracking Register (document record of who, what and when data is removed and returned to premises) should be maintained by the Contractor.   **All information held on the Contractor’s Personal Computers and Handheld Devices must be encrypted (see section 8)**  **Mobile Device Security**  The use of mobile devices is becoming more widespread and important to the successful delivery of DAERA services in line with the Department’s business strategy.  The loss of a mobile device and the subsequent loss of government data are considered by DAERA to be a security incident.  In addition to the laptop/mobile device and its data being unavailable for business use, there is also the potential for disclosure of personal or sensitive information.  The Department expects that contractors should regard such a loss of information to be more serious than the loss of the physical asset.  **Definition of a Mobile Device**  DAERA defines mobile devices as “laptops, mobile phones, smart phones, tablets, and approved external storage devices which can be used to access, store, process, transmit, discuss or record data electronically”.  **Minimum Security Requirements for Mobile Devices**  Mobile Device Security Policy require that, as a minimum:   * The information stored on any mobile device should be kept to the absolute minimum required for effective working; * All information is encrypted in transit over mobile communications channels and when at rest on the mobile devices themselves; * Mobile devices need to be appropriately secured and/or kept close to the owner/user at all times especially in public places; * Mobile devices must be stored in a physically secure location when not in use; * No mobile device should be left unattended, especially when in use; * Authentication credentials used with any encryption product such as tokens, passwords or other items necessary to access the information must not be stored with the mobile device at any time; * Users should treat all mobile devices and authentication credentials with the same care as they would their own valued possessions.   **Storing Data on Mobile Devices**  Where large quantities of data (meaning a quantity greater than 1,000 records), or any sensitive/personal data, is held on a mobile device, a risk assessment and privacy impact assessment must be carried out to consider the full impact of loss or compromise of the data.  **Dealing with Incidents and Loss**  Any lost mobile devices which may contain data must be reported immediately or as soon as reasonably possible to the Department. | |
| 10. | **Retention and disposal**   * All information required for the purposes of TB testing services will be retained by the Contractor for three years from receipt. * Thereafter all information must be securely disposed of. | |
| 11. | Security incidents or data breaches  * The Authority must be informed immediately in the event of a data breach or data loss involving any NIFAIS information. * All such incidents should be reported to:     TB Contract Manager,  Jubilee House,  111 Ballykelly Rd,  Limavady,  Co. Londonderry,  BT49 9 HP .  Email: [TB.CM@daera-ni.gov.uk](mailto:TB.CM@dardni.gov.uk)  In the event of a data loss incident, the Authority will instigate an investigation in line with the Authority’s Information Loss Handling Plan.   * The Contractor must fully engage in the resolution of an incident by assisting in the investigation being carried out by the Authority. | |
| 12. | Review/Termination of Data Sharing Agreement This Data Sharing Agreement will be reviewed 12 months after date of signing and yearly thereafter.  If any significant change takes place which makes the agreement an unreliable reference point, the agreement will be updated as needed and a new version circulated to replace it. Either signatory to this agreement can request an extraordinary review at any time.  The Authority reserves the right to terminate the agreement at any time if it believes that the Contractor is not adhering to the policies referred to in this agreement. As a result of this termination the Contractor will be required to securely dispose of any information owned by or obtained from the Authority. Access to NIFAIS may also be terminated. | |
| 13. | Indemnity The Contractor should be aware that Authority may ask them for a financial contribution towards any proceedings, should any claim or proceedings arise in respect of any breach of the agreement. | |
| 14. | Signatures I have read, understood and agree to abide by the terms and conditions of this agreement. All information received will only be used for the purpose defined and listed in the agreement.  Signed on behalf of the Authority  ----------------------------------------------------------  Name (block capitals):  Date:  Signed on behalf of the Contractor  --------------------------------------------------------  Name (block capitals):  Date: | |