Northern Ireland Ambulance Service
Health and Social Care Trust

BODY WORN VIDEO

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Data Protection Impact Assessment

This template is an example of how you can record your DPIA process and outcome. The Template follows the process set out in the ICO's DPIA guidance.

You should begin to fill out the template at the start of any major programme or project involving the use of personal data or, if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Project / Programme Name:	**Implementation of Body Worn Video Devices, incorporating audio (for use by ambulance service staff engaged in operational duties).**
Directorate:	**Medical Directorate**
Department/Location:	**Risk Management Department Northern Ireland Ambulance Service Site 30 Knockbracken Health Care Park Saintfield Road Belfast BT8 8SG**
Service or Project Lead completing the DPIA (name and contact details):	**Katrina Keating, Risk Manager**
Date DPIA commenced:	**28th June 2020**

Step 1: Assess the need for a DPIA

With a focus on Data Protection issues, in this section you should explain broadly the purpose of the processing and what the project aims to achieve? Clearly describe the intended effect on individuals, the benefits of the processing – for your service and more broadly?

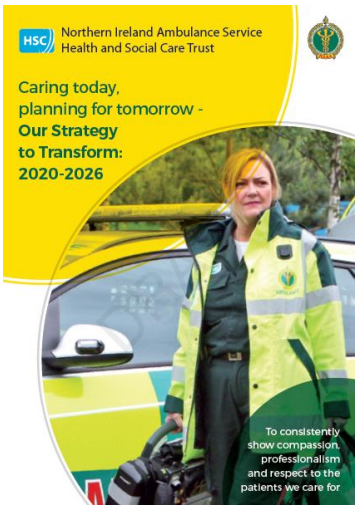
You may find it helpful to refer or link to other documents, such as a project proposal.

Also answer the questions below to help you identify the need for a Full DPIA.

<u>Briefly</u> describe the Project / Programme Objectives

It is an unfortunate fact that whilst caring for others, Northern Ireland Ambulance Service Health and Social Care Trust (NIAS) staff responding to emergency calls are exposed to violence and aggression on a daily basis. NIAS aims to reduce this risk to staff by the implementation of Body Worn Video (BWV) incorporating audio.

<u>Strategic Direction:</u>

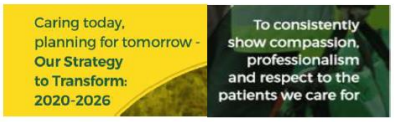


The Northern Ireland Ambulance Service has a strategic aim to improve staff health and wellbeing and reduce risk wherever possible. The introduction of BWV is designed to reduce the assaults upon staff with an associated reduction in sickness and cost.

<u>NIAS Strategy To Transform 2020 – 2026</u>

- *NIAS places a strong emphasis on staff wellbeing and safety. Staff safety is paramount and the Trust takes violence and aggression towards any member of staff whilst they are carrying out their role very seriously (page 26).*
- *We will continue to work with staff to understand the risks, review adverse incidents and revise the measures we take to do all that is reasonably practicable to protect our staff from these kinds of behaviours and actions (page 26).*

NIAS Corporate Plan 2020/21



NIAS Corporate Plan 2020/21

2.0 Our Workforce, Section 2.8, we will develop a comprehensive strategy for the management of aggression towards NIAS staff.

- Conduct risk assessments and needs analysis for physical security measures.
- Assess structure and resource requirements.
- Conduct a staff and public awareness campaign.
- Review the Corporate Management of Aggression Policy & Procedures.

Risk Assessment:

A number of risk assessments have been carried out with regards to violence and aggression across the service. These have been led by the Risk Manager in consultation with the Violence Prevention & Reduction Group (which includes an Ambulance Service Area Manager, Trade Union Representatives across all four Trade Unions, staff from Emergency Ambulance Control and Human Resources). All of these assessments have indicated that more needs to be done to protect NIAS staff. The implementation of BWV, incorporating audio (for use by staff responding to emergency calls) aims to enhance the safety of crews, reduce violence/aggression, and enhance public safety by acting as a deterrent.

Violence & Aggression Data:

Staff are asked to record any incidents of violence and aggression in the Trusts incident reporting system (DATIX). Within DATIX, incidents can be broken down in a number of categories with the following being those which are most frequently used:

1. Physical contact (actual assault).

2. Physical threat (no contact).
3. Psychological abuse.
4. Sexual.
5. Verbal abuse.
6. Verbal abuse with racial content.

1. Physical Contact / Actual Assault – over the past five years, NIAS staff have been physically assaulted with items including a knuckle-duster, syringe, sledgehammer, glass bottle, stones, ashtray, crowbar, desk fan, snooker cue and balls, 0_2 cylinder, bag of cement, tomahawk hatchet, cups, scissors, fire extinguisher, Stanley knife, razor blades, hammer etc.

   Physical assaults with weapons continue to increase. In 2019/20, twelve out of the 23 weapon incidents involved knives, i.e. around 50%.

Year	Total Assaults	Physical Assaults	Assaults With Weapons	Physical Assaults	
				Ambulance Care Attendants	Accident & Emergency
2016/17	451	192	4 (2%)	8	171
2017/18	487	191	9 (5%)	13	161
2018/19	455	171	27 (16%)	2	160
2019/20	463	152	24 (16%)	7	145
2020/21	604	208	46 (22%)	13	195

2. Physical threat / no contact – examples include staff being held against their will in domestic premises, threatened with sticks, being swung at, attempts to bite, threatened with dogs, threats to kill (including details as to how), squaring up behaviours, pointing in face, lunged at with scissors / knives etc. With regards to firearms, three examples are as follows:

   - Crew attended scene and the patient had a handgun sitting on his lap (subsequently found to fire ball bearings).
   - Patient armed and PSNI made the scene safe.
   - Crew disarmed a member of the public who forced their way into a property.

3. Psychological abuse – Examples in this area include those of a very personal nature suggesting that the perpetrator knows where the person lives, threats to their family, insinuations, threats to kill and sectarian comments. Also, during the COVID-19 pandemic (March 2020 forward) some service users have been spitting at staff with a view to deliberately causing harm by intentionally spreading the disease. This is an extremely worrying trend and these events have a lasting psychological impact on those involved, see links to media reports[1],[2].

[1] **https://www.itv.com/news/utv/2020-06-08/35-attacks-on-ni-ambulance-crews-in-just-one-week/**
[2] **https://www.bbc.co.uk/news/uk-northern-ireland-52995752**

4. Sexual – staff have been sexually assaulted repeatedly whilst caring for patients, for example hands inappropriately placed on staff, suggestive comments, inappropriate exposures and unwanted touching. Please note that both male and female crew members are being targeted equally in this area.

5. Verbal abuse – of a grossly offensive and extreme nature, shouting close to the face, threats of a sectarian nature, threats to kill etc.

6. Verbal abuse with racial content – use of grossly offensive verbal abuse of a racial nature.

7. Biological Agents / COVID-19 assaults (also see 3 above)

   The following incidents have been recorded:

   - Squeezed bicep to squirt blood around deliberately (HIV positive).
   - Deliberate spreading of blood onto crew during COVID-19.
   - Instances of COVID-19 assaults, i.e. members of the public / service users deliberately spitting or coughing at ambulance crews during the pandemic in an attempt to infect them with or cause them alarm / impact on their mental health impact. Ambulance staff also witnessed PSNI being spat at.

8. Miscellaneous Aggression Incidents

   The following incidents have also been recorded:

   - Punching equipment.
   - Tearing apart equipment, for example Corpuls defibrillator worth 17K.
   - Deliberate urination on equipment and vehicles.
   - Deliberate defecation in vehicles.

Moral / Legal / Financial:

NIAS is required to ensure the safety of its staff, both from a legal and a moral perspective. Under the Health and Safety at Work (Northern Ireland) Order 1978, and the Management of Health and Safety at Work Regulations (Northern Ireland) 2000, NIAS is required to carry out suitable and sufficient risk assessments to ensure that adequate control measures are in place. NIAS must ensure it takes all measures reasonably practicable to ensure the safety of its staff.

Staff who have suffered as a result of violence and aggression usually require varying periods of time off work. This reduces the resources available, and service delivery to the wider public suffers as a result. It also increases the operating costs due to having to fund alternative staff to cover.

Legislative Compliance:

If implemented, BWV devices will be able to capture both video and audio images and NIAS will ensure compliance with the Data Protection Act 2018

and the UK General Data Regulation. Other supporting guidance that will add legislative compliance include; Technical Guidance for Body Worn Devices, Home Office, July 2018; Encryption Guidance, Information Commissioner's Office; CCTV Code of Practice, Information Commissioner's Office, May 2014; Guide to Law Enforcement Processing (Part 3 of the DP Act 2018), Information Commissioner's Office, 2018; Surveillance Camera Code of Practice, Surveillance Camera Commissioner, June 2013. We will fully consider data protection obligations including:

- Utilising of BWV must be lawful and fair.
- Obligation to be transparent about recording.
- Minimising the amount of personal data recorded.
- Maintaining security and integrity of recording.
- Responding to data Subject Requests and ensuring that processes are in place to manage rights for an individual recorded by BWV devices including restriction of personal data.

NIAS will further ensure:

- Standard operating procedures are in place to guide BWV users on when to activate and deactivate a recording.
- BWV users will be made aware of their device's potential to capture large amounts of intended sensitive information.
- BWV users will be made aware of the need to consider ending a recording or temporarily covering the camera or microphone or both to minimise the capture of sensitive information.
- The need for greater discretion when recording in special locations.

The operational use of BWV is proportionate, legitimate and necessary; it is proposed that it will be only used when deemed necessary for the purposes of violence reduction, by trained staff in accordance with policy, procedures and legislation.

Does the project or change in process involve any of the following?	Yes	No	Explain the reason for your 'answer (whether Yes or No) in a few words or a sentence.
Collection			
Collecting **new information** about individuals; a new way of gathering personal information; or establishing a new way of identifying individuals.	☒	☐	Yes new information will be collected in the form of audio and video footage if BWV is implemented. CCTV is already in operation in ambulance vehicles and stations but only video footage is recorded. It is recognised that audio recording is a greater infringement of privacy for both staff, patients and the wider general public, however, the inclusion of audio improves the quality of the evidence captured, where the capture of video evidence alone may not be sufficient. In some circumstances, the presence of only video evidence, can fail to adequately provide the full context of an incident. Another aspect of the inclusion of audio information is that, in some instances, the camera itself may not be pointing in the direction of the main incident but the audio will still be captured. This has the advantage of protecting all parties to ensure that the actions of the staff member were in accordance with the law and Trust policies. The legal basis for collection of BWV information is that processing is necessary for our purpose of the legitimate interests pursued by the Data Controller (Northern Ireland Ambulance Service), under the UK General Data Protection Regulation Article 6(1)(f). Our legitimate interest so in order to: • Protect staff, patients and third parties. • The use of BWV by NIAS staff will support the relevant authorities in the apprehension and prosecution of

			offenders and provide evidence to take criminal or civil action in the Courts. • May assist in providing a deterrent effect and reduce unlawful activity. • Help provide a safer environment for our staff. Benefits would include: • First accounts from victims, suspects or witnesses. • Identification of a person. • Direct conversations with a member of the public. • Decisions and actions of the BWV user. • Physical and mental state of people. • Actions of people. • Prevailing atmosphere during an incident. • Location of evidence. The collection of new information on BWV <u>may</u> include: <u>NIAS Staff and Emergency Personnel</u> BWV will collect personal information on ambulance staff and other emergency personnel on scene that will enable: • Visual and verbal identification. • Private conversations and comments. • Personnel in a distressed nature. • Information displayed on personal mobile phones. • Shoulder or other identification numbers. • Name badge or ID pass. <u>Members of the Public/Patients</u> • Visual identification. • Verbal identification. • Private conversations and comments. • People in a distressed state. • Features of a person's vehicle.

			• Features within a person's home. • Features of a person's workplace. • People in a state of undress. <u>Private Home</u> • Details of children whether present or not. • Domestic order of property. • Occupants in a state of undress. • Emotionally distressed occupants. • Identification of occupants. • Personal medical products. <u>Hospital</u> • Patients in physical distress. • Personal medical confidentiality. • Patients in a state of undress. • Emotionally distressed patients or visitors. • Identification of patients, staff or visitors. • Location of pharmaceutical products. <u>Residential Care</u> • Building access codes. • Occupants in a state of undress. • Details of vulnerable people whether present or not. • Personal medical products. <u>Police Station</u> • Risk of building codes. • Details of police investigations. • Identification of personnel. • Identification of visitors. <u>Prison</u> • Building access codes. • Building layouts. • Identification of personnel. • Identification of inmates. • Security protocols.

			Bank • Building access codes. • Building layouts. • Identification of personnel. • Security protocols. Place of Worship • Intrusion of private contemplation. • Intrusion of private ceremonies. • Identification of people attending group sessions. NOTE The resulting consultation may limit use in some areas.
Use or Disclosure			
Using an individual's **personal data already held in an existing system** (manual or electronic) **for a new purpose or in a new way**	☐	☒	No. Data in this area is not already held in this format.
Disclosing or sharing personal information with organisations or people who have not previously had routine access to it	☒	☐	In certain circumstances, (investigations, serious or criminal incidents) we may need to disclose BWV footage for legal reasons. When this is done there is a legal requirement for the receiving organisation that has received the information to adhere to data protection principles. BWV footage evidence may be released to the PSNI for the reasons of crime prevention and public safety/in the event of a criminal act. This is released to PSNI to support a police investigation. NIAS already has existing protocols with PSNI in terms of the release of information in line with data protection legislation as follows: Section 32 of the Police (NI) Order Act 2000 states it shall be the general duty of Police Officers to protect life, property, preserve order, prevent the commission of offences and where an

			offence is committed to take measures to bring the offender to justice. The Data Protection Act 2018 defines personal data as any information relating to an identified or identifiable living individual. The Data Protection Act (2018) and the UK General Data Protection Regulation (UK GDPR), allows for the disclosure of personal data to Police when the purpose is to prevent and detect crime: (a) Article 6 of UK GDPR allows for the general processing of personal data when it is necessary for (but not limited to), compliance with a legal obligation; the protection of the vital interest(s) of the data subjects, or another natural person; or a task carried out for the public interest which includes but is not limited to, the administration of Justice under Article 8{a) of the Data Protection Act (2018). *(b)* Article 9 of UK GDPR allows for processing in relation to Special Category data where it is necessary for {but notlimited to) the protection of the vital interest(s) of another natural person; or for reasons of substantial public interest as detailed in Schedule 1 part 2 of Data Protection Act (2018) which includes but is not limited to, *'preventing or detecting unlawful acts'* and *'safeguarding children and of individuals at risk'.* *(c)* The processing of personal data, including Sensitive Processing, by another Competent Authority may be processed lawfully when strictly necessary for a law enforcement purpose as per Part 3 of the Data Protection Act (2018). Law enforcement

			purpose is defined as *'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention of threats to public security'.* A Competent Authority is a body listed in Schedule 7 of the Data Protection Act (2018) and has alaw enforcement function, e.g. a local council, Probation Board, other police forces etc. Special Category data and Sensitive Processing means data revealing racial or ethnic origin, political opinions, religious, philosophical belief, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation (Article 9 of UK GDPR and S.35(8) Data Protection Act (2018). Human Rights Act 1998 Article 8 - right to privacy. This request is consistent with Article 8(2) prevention of disorder or crime. When capturing information on BWV devices, NIAS will only do so to fulfil a legal purpose such as sharing with PSNI when an offence as or is perceived to have taken place or the member of staff feels under threat. The use of this equipment is to support the relevant authorities as necessary in the prevention and detection of crime and provide public disorder. When information is captured, it will be firstly assessed as to whether it constitutes evidential or non-evidential material. Any material, which is deemed as evidential could then be shared with the Police. On rare occasions, BWV material could be released by PSNI, to the media if there is a genuine need to do so e.g.

			identification of an unknown suspect in relation to a serious effect. Other relevant authorities that BWV could be shared with would include the Police Ombudsman, Health and Safety Executive, Directorate of Legal Services or other organisations as necessary in order to support the prevention and detection of crime or investigations associated to same.
Matching or linking with personal information held by different organisations or in different datasets e.g. combining, comparing or matching personal data obtained from multiple sources	☐	☒	The data will not be matched or linked within NIAS. If BWV footage is released to PSNI they may be able to identify, for example, an attacker from information they already hold.
Storage, Security and Retention			
A change in the way personal information is managed, stored or secured (e.g. new database, new location, cloud storage)	☒	☐	Yes the introduction of BWV into NIAS would be new technology. NIAS will consider the physical security of the BWV on NIAS personnel, protecting data on BWV devices i.e. encryption, transferring the data to a local server on site and asset management of BWV devices. Data will only be captured during an act of aggression when the staff switch the BWV devices on – the device is not constantly storing data. The BWV is activated when a record button is pushed by the staff member. A light will then show the BWV recording. Staff will activate their cameras at the start of an incident and under normal circumstances will continue to record until it's no longer 'proportionate or necessary'. Any footage on the BWV will be stored on each individual device until the data is transferred off the device to a secure local server. Normally this will be mean by the end of the ambulance staff members' shift.

			Docking stations and dedicated software will be evident in each Ambulance Station across Northern Ireland. Location of docking stations will be in secure and accessible locations. Once the BWV has been docked, the data transfer process will be automated and transferred to the server. This will only transfer data if the record button has been pressed on the BWV device and data is held during the shift the ambulance staff were undertaking. It is envisaged that devices will also have a backup to allow for data transfer via a USB cable or secure wireless connection. All recordings will be erased from the individual device once the data has been transferred. • Footage provided to PSNI, Police Ombudsman, Health and Safety Executive or other statutory agencies for criminal investigation; Trust copy securely destroyed after 2 years. • Footage required for internal/external employee related investigations, Health and Care Professional Council (HCPC), personal injury claims (and identified as secondary processing); securely destroyed after one year. • Unmarked footage; securely destroyed after 31 days. The rationale for any retention beyond this timescale may include circumstances where there is a secondary use of the BWV and may be in such circumstances including employee related investigations, complaints, HCPC personal claims management etc. Secondary use of any BWV footage for such investigations will be used where necessary for the purposes of preventing, investigating, detecting or prosecuting criminal offences including

			safeguarding against threats to public safety. In circumstances where the information is evidential, master and working copies are created and retained. At the conclusion of any investigation/review or complaint, there is a requirement to hold the data in accordance with Trust retention schedules. Where information is shared with the Police or other body, they will be responsible for the secure retention and destruction of the data in line with their policies. The captured images and audio cannot be replayed on the BWV device by the individual staff member. All video files from BWV devices will have a unique reference to ensure the data can be stored within a structured filing system enabling future search and retrieval. Technical metadata would be applied to BWV devices automatically and this will include start time and date, length of recording, image resolution, frame rate, file size, location information such as GPS data. Business metadata will also be stored which may include description of content, type of incident, data retention periods, associated video files etc. Audio and video footage will be managed in line with the Trust's Information Governance framework including Retention and Disposal Schedule and ICT protocols. The Risk Manager will work with the Head of Information and ICT to ensure new software is compliant with HSC security and information governance requirements.

Summary of Initial Assessment and need for a Full Data Protection Impact Assessment	**Click box to select relevant option**
I have answered **Yes to one or more of the above questions** I acknowledge that further consideration needs to be given to any potential data privacy risks that might be associated with this new project or change in process. Risks may arise due to the level and/or sensitivity of the personal data involved; the significance of the change in process; or the potential impact on individuals whose information is to be processed. I agree that **a full Data Protection Impact Assessment is necessary** to help me address the data protection issues associated with this new process. **Proceed to Step 2**	☒
I have answered **No to ALL of the above questions**. I believe that there is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or that the risks are low and fully mitigated. On this basis I believe that **a full Data Protection Impact Assessment is not required** **Proceed to Step 6 to sign off and record the outcome**	☐

Full Data Protection Impact Assessment (DPIA)

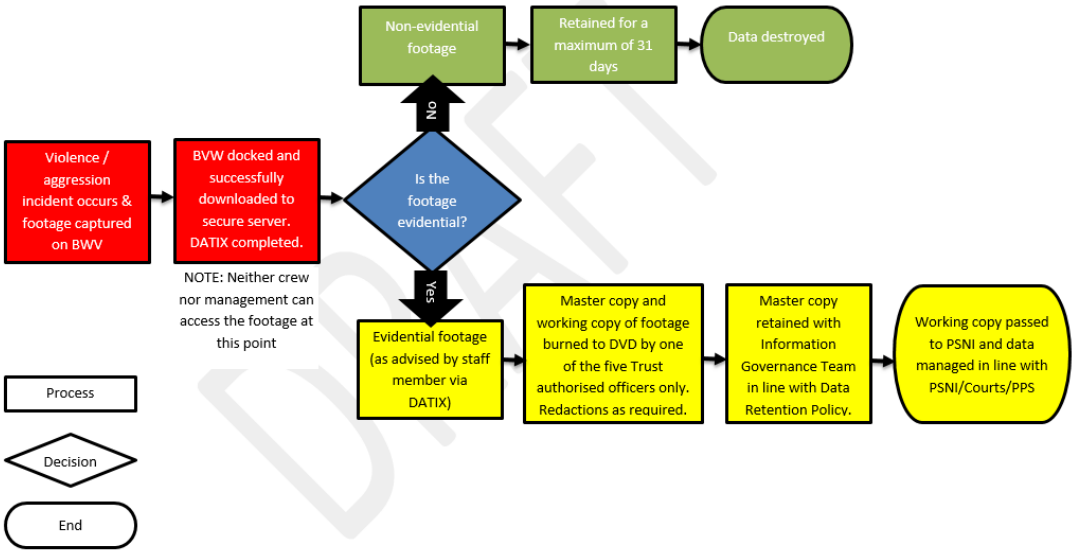
Step 2: Describe the processing

Describe the nature of the processing:

In this section please provide details of the data flow(s) for all the stages of the process that involve sharing or receiving personal data. Your data flow should clearly outline what data you are processing, all the uses of the data and with whom the data flows to and from (explaining if it is 'one-way' or 'two-way' data sharing). In order for Information Governance to comment or advise you on your DPIA a data flow map should always be completed in the first instance. The following questions should inform your data flow.

It may help to include a data flow diagram or flow chart.

FLOW OF INFORMATION – DATA CAPTURED BY BODY WORN VIDEO FOLLOWING AN INCIDENT OF VIOLENCE / AGGRESSION



List the Personal Data collected at each stage of this process? Please note that personal identifiable data may also include any one of the following

Name, address, full postcode, date of birth, health and care number, hospital number, email address (this list is not exhaustive)

NIAS hopes to implement BWV cameras that are capable of capturing both moving images and audio information. They would be worn by uniformed operational ambulance service staff attending calls.

The audio and visual images captured shall be associated with acts of verbal and physical aggression and violence, and captured in accordance with

information, instruction and training. It is not intended to capture any sensitive personal data. But is recognised that this may occur depending on each individual situation as BWV devices not only record both video and audio but they employ wide lenses that captures a broad field of view. This can result in the capture of much larger amounts of personal information than the user intended.

Collateral intrusion – As above, it is possible however that the camera field of view may include individuals (members of the public, staff, etc.) not directly involved in the incident, i.e. bystanders resulting in individuals being recorded by devices without them being fully aware. This is known as collateral intrusion and in this context extends to the capturing of the movements and actions of other persons, not involved in an incident, when this equipment is being used. It is inevitable that in some circumstances this will occur, albeit staff will be trained to ensure that wherever possible, the focus of their activity is on the subject of attention. In circumstances where citizens are captured in any video or audio information and they are unrelated to any offence under investigation, their identities will be protected and anonymised especially should the matter be presented to a court. Any requests received under subject access will also be managed in line with data protection requirements as they are entitled to their personal data but are not entitled to another person's personal data, especially if this could cause harm. It is also recognised that once information is released, it is not possible to restrict or control how the data subject shares the information provided to them. It is recognised that information from a BWV could be posted by the recipient on Social media and may attract views from those not involved in the incident.

Personal data collected will vary from situation to situation as the BWV device will only be turned on by the staff member if required due to an escalation in an incident. The incident could happen in many locations e.g., public area, domestic property, work location, in the back of the ambulance, in a Police station etc.

Personal information collected could include patient name, address, data of birth, clinical condition of patient, date of birth, next of kin details, GP contact details etc.

Specific examples also could include collecting personal information:

NIAS Staff and Emergency Personnel

- Visual and verbal identification of staff member by name.
- Private conversations and comments.
- Personnel in a distressed nature.
- Information displayed on personal mobile phones.
- Shoulder or other identification number.
- Name badge or ID pass.
- Vehicle registrations/make and model of car/ambulances.

Private Home

- Details of children whether present or not.
- Domestic order of property.
- Occupants in a state of undress.
- Emotionally distressed occupants.
- Identification of occupants.
- Personal medical products and medication.

Police Station

- Risk of building codes.
- Details of police investigations.
- Identification of personnel.
- Identification of visitors.

Prison

- Building access codes.
- Building layouts.
- Identification of personnel.
- Identification of inmates.
- Security protocols.

Bank

- Building access codes.
- Building layouts.
- Identification of personnel.
- Security protocols.

Place of Worship

- Intrusion of private contemplation.
- Intrusion of private ceremonies.
- Identification of people attending group sessions.
- Religious or philosophical beliefs.

NOTE The resulting consultation may limit use in some areas.

No staff member will be issued a BWV device without having completed the relevant training package.

List any Special Category Data you will be processing?

[The following categories would be classified as special category - Health Data, Genetic Data, Biometric data for purposes of identification, data concerning a natural persons sex life or sexual orientation, racial or ethnic origin, political opinion, trade union membership, religious or philosophical beliefs]

If yes which of the above categories does it fall under?

Health data, data concerning a person's sex life or sexual orientation, racial or ethnic origin, political opinion, religious or philosophical belief may be inadvertently captured in the event that a member of the public assaults a member of staff during treatment and it may be the video and audio recording collects levels of this information.

How do you intend to share the Personal Data / Special Category Data securely? What methods will you use to protect the information in transit? Have you consulted with your IT department?

Policies, procedures and a training plan will be put in place to support any introduction of BWV devices and the sharing of personal data/special category data securely. This will include data recorded by BWV devices, measures to safeguard BWV data including physical security of devices, encryption, protecting data on the BWV devices, transferring data to a local server, tagging and organising data, asset management of BWV devices. Protocols for distributing or sharing BWV will be in place and will cover sharing data for a legitimate purpose i.e. PSNI, Police Ombudsman, Health and Safety Executive etc. and will include processes for releasing data for subject access request which will include visual data redaction, audio data redaction and output data.

BWV footage captured for the purposes of violence and aggression may also be shared internally, for circumstances where there is a desire to review allegations made under a complaint, disciplinary process or Serious Adverse Incident investigation. This BWV footage will only be shared if appropriate to do so, and will be reviewed on a case by case basis.

Data will only be captured during an act of aggression when the staff switch the BWV devices on, as the device is not constantly storing data. The BWV device will be constantly operating but will only **store** data if the record button is pushed by the staff member. If record is pushed, the BWV device will buffer up to 60 seconds prior to the record button was used. Staff will activate their cameras at the start of an incident and under normal circumstances will continue to record until it is no longer 'proportionate or necessary'.

Any footage on the BWV will be stored on each individual device until the data is transferred off the device to a secure back office system/server. Normally this will be carried out at the end of the shift by the ambulance personnel. Docking stations and dedicated software will be evident in each Ambulance Station across Northern Ireland. Location of docking stations will be in secure and accessible locations. Once the BWV has been docked, the data transfer process will be automated, encrypted and transferred to the server. This will only transfer data if the record button has been pressed on the BWV device and data is held.

Devices will also have a backup to allow for data transfer via a USB cable or secure wireless connection. All recordings will be erased from the individual device once the data has been transferred. The captured images and audio cannot be replayed on the BWV device by the individual staff member.

The Trust has an ICT resource and expertise as part of project team. The BWV is not yet implemented but protecting data on BWV devices if and when a supplier is appointed will be of priority. This will include protocols on accessing risk factors associated to storage media options e.g. removable media or non-removable media, accidental loss of media, interference on data physical damage to media, compromise to continuity, flexibility of data transfer options. Encryptions will be fully accessed to review direct access to data, data or metadata that is scrambled exclusive to a supplier, same access code or key to encrypt and decrypt data etc. Risks will include data accessible by an unauthorised party, sharing data with external agencies etc.

It is likely that devices will have radio frequency identification (RFID) and booked out to an individual from a pool of devices. The device would be encrypted and there is a limited amount of captured information stored on the device's internal memory and requires specific docking facilities to access the footage. In addition it is important to note that the recording itself is encrypted, as it records, not the device. AES256 standard. Only the software can decrypt it, so when it is uploaded to Trust storage systems, the recording remains encrypted. Depending on supplier, it is likely that the software decrypts the recording and stores separately, therefore two versions exist, an encrypted and a decrypted. The software may also be able to auto purge all decrypted recordings. Footage will only be accessed by one of the five authorised and nominated Trust staff via PCs with personal logins, and only held past 31 days if it is deemed as evidential.

Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged, i.e. footage will be supplied for evidential purposes only. It will be decrypted using the software and emailed to IT requesting it to be put on a password protected DVD/CD. Footage must be requested by authorised police staff or other statutory agencies with legitimate powers to access the information. Immediate supply for life/death, detection of crime incidents will be provided in written request of a police officer of at least Inspector rank. In all cases a Form 81 will be required from PSNI to release BWV footage. Master copy will be retained securely on-site with the Information Governance Team.

If applicable, how will the receiving service/organisation use the data? How will they hold it securely? Do they intend to share the information with other organisations or services? If so, for what purpose?

BWV and audio data evidence may be released to the PSNI for the reasons of crime prevention and public safety/in the event of a criminal act i.e. that a NIAS staff member has been attacked verbally or physically by a member of the public. In circumstances other organisations with statutory powers may also been able to access this record including the Police Ombudsman, Health and Safety Executive, HCPC etc to support their own investigations.

The release of any BWV footage is for evidential purposes, so that it can be used as evidence in a Court of Law or other legal proceedings.

Any releases of BWV footage are to public sector organisations who have to comply with data protection legislation as part of their day to day work and they will have their information governance framework in place to support this which will including policies, procedures and training protocols to their own staff. These organisations will also be registered with the Information Commissioners Office. Any releases third party releases i.e. subject access request (SAR) will be managed appropriately in line with Data Protection legislation and supported by Information Governance Policies and Procedures that exist within the Trust. The SAR may include the release of the BWV footage as well as other supplementary information. While a Data Subject is entitled to their personal data they are not entitled to another person's personal data especially if this could cause that person harm. Redaction and pixilation of BWV will used where required, so that data released under a SAR relates only to that person.

Any internal/external release of BWV footage to support secondary processing for such investigation as employee related investigations, HCPC, personal claims etc will be managed in line with data protection protocols.

If applicable, what Personal Data / Special Category Data will you receive from other organisations or departments? What format will the information be received (manual paper information/ electronic information)? How will it be secured in transit? How will you store the data securely? Who will have access to it?

NIAS will be releasing data in line with data protection protocols. No data will be received, therefore not applicable.

Step 3: Consultation process

Have you considered the impact of the new process or system on all stakeholders? Who have you consulted with, both internal and external stakeholders.

Please justify why it's not appropriate to do so.

NIAS recognises that there are a large number of stakeholders with an interest in how BWV devices will be deployed and utilised by NIAS. Consultation is a key element of the PIA process. This will help NIAS gauge the reaction of the public to the operational deployment of BWV devices and address any concerns they may have in this regard. The process can be summarised as follows:

- Combined DPIA, EQIA, HR screening and Rural Needs into one document along with proposals about the whats, hows and whys of BWV for public to consult on in the spirit of co-production
- Easy-read version of same provided (other language translations can be provided on request).
- Animations, infographics & leaflets to inform public about the consultation (Communication Team involvement). Any Easy-read, animations and infographics will have consistency, will require coordination between agencies.
- 10 weeks of consultation – publicise on website (dedicated area), SharePoint, social media (internal & external). Consideration will be given to print media, local news outlets, local radio and libraries (Communication Strategy) and consideration to direct mail to relevant persons on HSC consultee list / Stakeholders Forum list (c. 350 organisations and individuals).
- Potential to directly contact specific groups and organisations that we identify as potentially having significant interest (e.g. Human Rights Commissioner).
- Signal boosts that the consultation is live and open (Communication Team).
- Equality & PPI Team / Risk Team will maintain consultation logs and compile responses thematically for consideration (this could be incorporated into project plan).
- Hold a minimum of two public meetings (remote) – one in week 3 and one in week 8 – invite specific groups as above and anyone who has responded to the consultation (meetings can be supported by video sign language interpreters through regional contract).
- Meet individually with people who have raised specific issues that could be incorporated into proposals and potential policy and procedure in a co-design/co-production manner
- On completion the project lead will have to respond to the consultees with mitigations, changes and a final proposal. This could include draft policy and procedure if we are at that stage.

- On approval of business case and prior to moving to procurement, consultees should be given another opportunity to review the final direction of the project.

Members of the public – as above a full public consultation will be carried out and NIAS will provide the following:

- A published point of contact for information, complaints and concerns.
- NIAS Privacy Notice will be updated.
- Added to NIAS information asset register.
- Added to risk registers as appropriate.
- The required CCTV signage.
- Training for staff in order that they can confidently engage with members of the public on the matter.
- Appropriate Policies, Procedures and Training will be developed and implemented.

NIAS Operational staff – all of the above public information. Staff will be contacted to provide an expression of interest to join the Project Team should the project be agreed. Staff will be kept informed as the project progression via recorded soundbites, memos, newsletters, updates to NIAS Websites and SharePoint, via Trade Union colleagues etc. Staff will be advised to raise any concerns immediately with either line management or a member of the Violence Prevention & Reduction Group.

NIAS Management / Trust Board / SIRO / ICT etc. – following consultation, a business case supporting the procurement of BWV devices will be presented to Senior Management. Information Governance and Equality staff have been engaged and helpful from the outset (February 2020). Regular updates will be provided on the development of the PIA and associated project timescales. BWV Policy, Procedures and Standard Operating Procedures will be developed and undergo full consultation and be presented to various groups and committees to Trust Board level.

Existing governance reporting and assurance structures will be utilised in order to ensure due governance, for example presentation to Violence Prevention & Reduction Group, Health and Safety Committee, Information Governance Group, Informatics Assurance Group, Audit and Risk Assurance Committee and Trust Board. A Project Team will be established with the normal associated project arrangements including regular meetings, agendas, action points, progress plans etc.

NIAS Trade Unions / Staff Representatives etc. – have been involved in all stages of the process. NIAS Trade Unions are members of the Violence Prevention & Reduction Group, and were contacted via email on the 12th June 2020 and asked to nominate members for the Project Team. TU colleagues will be working in partnership with NIAS management on the implementation of BWV in NIAS.

Department of Health / Commissioners / HSCB – will be contacted directly in order to solicit their views as part of the development of the business case, and on an ongoing basis.

NHS England & NHS Improvement (Security Lead) – contacted and liaison ongoing with regards to route to ongoing pilots in Great Britain, procurement, strategy and framework.

PSNI / PPS / Courts / Regulators etc. - will be contacted directly in order to solicit their views as part of the development of the business case, and on an ongoing basis.

Health and Social Care Trusts - will be contacted directly in order to solicit their views (staff entering EDs etc.).

Representative of Commercial Premises (shopping centres/hospitality, private nursing homes) – will be included in order to solicit their views.

Representatives of private business (farming, manufacturing etc.) – will be included in order to solicit their views.

Representatives of Lesbian, Gay, Bisexual and Transgender (LGBT) groups – will be included in order to solicit their views.

Representatives of groups with particular religions or beliefs – will be included in order to solicit their views.

Representatives of Black, Asian and minority ethnic (BAME) groups – will be included in order to solicit their views.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures

In order to show that your processing is 'necessary' for a specific purpose, you must have a valid lawful basis in order to process personal / special category data in compliance with Article 6 and Article 9 of UK GDPR. You will need to consider what your lawful basis is for the collection and processing of personal/special category data at each step of the data flow

What is your UK GDPR lawful basis for processing (see Appendix 2 below and consult your IG department)?

It is an unfortunate fact that, on a daily basis, Northern Ireland Ambulance Service Health and Social Care Trust (NIAS) staff are exposed to violence and aggression whilst saving lives and providing medical treatment / helping others.

Health and Safety at Work (Northern Ireland) Order 1978 and the Management of Health and Safety at Work Regulations (Northern Ireland) 2000 – NIAS is required to assess risks to staff and ensure that adequate control measures are in place. A regular review of the corporate risk assessment with regards to violence and aggression is carried out by the Managing of Aggression Group, and the associated action plan is regularly updated. The most recent review was led by the Risk Manager in consultation with the Violence Prevention & Reduction Group which includes an Ambulance Service Area Manager, Trade Union Representatives across all four Trade Unions, staff from Emergency Ambulance Control and Human Resources. This risk assessment has clearly indicated that more needs to be done to protect NIAS staff. The ambulance environment is challenging in that there is very limited scope for the implementation of control measures such as improving the workplace space, lighting security etc., therefore alternative controls such as BWV must be considered.

Operational staff will only deploy BWV recording against the defined operational requirements (where there is a risk of violence, aggression or assault or criminal acts against staff) and we need to ensure that the use is proportionate, legitimate, necessary and justifiable. In every case where the BWV is activated, the staff member involved must be prepared to justify its use.

The Data Protection Act 2018 defines personal data as any information relating to an identified or identifiable living individual and UK GDPR allows for the disclosure of personal data to, for example, to Police when the purpose is to prevent and detect crime.

The legal basis for collection of BWV information is that processing is necessary for our purpose of the **legitimate interests** pursued by the Data Controller (Northern Ireland Ambulance Service), under the UK General Data Protection Regulation Article 6(1)(f) – Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third

party, except where such interest are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is child.

Our legitimate interest so in order to:

- Protect staff, patients and third parties;
- BWV will assist, for example, PSNI in the apprehension and prosecution of offenders and provide evidence to take criminal or civil action in the Courts;
- Assist in providing a deterrent effect and reduce unlawful activity;
- Help provide a safer environment for our staff.
- Processing carried out by public authorities in the performance of their duties.

We are seeing increases on attacks on ambulance staff. Scenarios are continually arising when an attack on ambulance staff member occurs and the PSNI are able to arrest the individual but then may be released under investigation, while enquiries continue. If ambulance staff had been using BWV devices when they had been attacked, then the process of investigating the offence could be more effective and may result in a successful prosecution. It would provide first accounts from victims, suspects or witnesses; it would aid the identification of a person; audio would show the direct conversations with the members of the public; it would show the decisions and actions of the NIAS staff member to use the BWV; the physical and mental state of people; demeanor of people; actions of people; prevailing atmosphere during an incident, incident location and record of criminal activity.

If PSNI (or other statutory agencies with powers of access) had timely access to BWV at the early stages of an investigation then the Officer could replay the footage to a suspect during an initial interview (along with other available evidence including 999 calls, statements of evidence from ambulance staff etc.). NIAS has duty to protect frontline ambulance staff. BWV device implementation is vital to support this and is invaluable as evidence to increase guilty pleas.

Article 9 of UK GDPR allows for processing in relation to Special Category data where it is necessary for {but not limited to) the protection of the vital interest(s) of another natural person; or for reasons of substantial public interest as detailed in Schedule 1 part 2 of Data Protection Act (2018) which includes but is not limited to, *'preventing or detecting unlawful acts'* and *'safeguarding children and of individuals at risk'.*

Pursuant, Article 10 of UK GDPR allows the processing of personal data relating to criminal convictions and offences.

NIAS fully understands that the utilisation of BWV cameras must be lawful and fair. All processing of personal data which does fall under the remit of the UK GDPR must be fair and lawful. This means we must have an appropriate legal basis or justification, for using BWV as required by Article

6, 9 and 10 of the UK GDPR and as outlined above. Any footage recorded can only be processed for purposes that are otherwise lawful and fair towards affected data subjects. Any BWV devices implemented will not be unduly detrimental, unexpected, misleading, or deceptive to individuals who are recorded and protocols will be put in place to support this. NIAS fully supports this stance that BWV devices are necessary for achieving the purpose of reducing unprovoked attacks on ambulance personnel by members of the public but also understands that we have to have clear policies, procedures and training programmes in the use to introduce them into the Ambulance Service. We will ensure that we act with integrity and transparency with their use. This offers protection for both the public and NIIAS frontline staff. We will ensure the existence of appropriate safeguards, which may include encryption or pseudonymisation.

It is further recognised that consent will not be an appropriate legal basis for the use of BWV devices as gathering the consent of each person recorded would not be possible or practical. In the event that someone requests that the BWV be switched off, the staff member may advise the person that:

- Any non-evidential material is only retained for a maximum of 31 days.
- This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law.
- Recorded material can be accessed on request in writing in accordance with the DPA, unless an exemption applies.

The BWV operator will consider on a case-by-case basis whether or not to switch the BWV off. There should always be a presumption to record if the 'need to address a pressing social need' has been achieved unless the circumstances dictate otherwise. A colleague failing to record an incident may be required to justify the actions as vigorously as any colleague who chooses to record a like encounter. In all cases, recording can only be justified when it is relevant to the incident and necessary in orderto gather evidence.

Other compliance protocols and supporting legislative frameworks:

- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) Northern Ireland 1997 – NIAS is required to notify their enforcing authority in the event that an accident at work affects any employee, resulting in death, major injury, on incapacity for normal work for three or more days. This includes any act of non-consensual physical violence done to a person at work and these are reported regularly by NIAS. In the case of breaches of health and safety legislation, the Health and Safety Executive for Northern Ireland (HSENI) and/or local authorities are responsible for enforcement.

- Justice Act (Northern Ireland) 2016 – Offence of assaulting ambulance workers etc.

  (1) A person commits an offence if he or she assaults—

a) an ambulance worker in the execution of that ambulance worker's duty;
b) a person who is assisting an ambulance worker in the execution of that ambulance worker's duty.

(2) "Ambulance worker" means a person who provides ambulance services (including air ambulance services) under arrangements made by or at the request of—

a) the Northern Ireland Ambulance Service Health and Social Care Trust,
b) St. John Ambulance (NI),
c) the British Red Cross Society, or
d) the charity registered in the Republic of Ireland known as the Order of Malta Ireland.

(3) A person guilty of an offence under subsection (1) shall be liable—

a) on summary conviction, to imprisonment for a term not exceeding 6months or to a fine not exceeding the statutory maximum, or to both; or
b) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

- European Convention of Human Rights, European Convention on the Rights of the Child and Human Rights Act 1998 – In general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's (including a child's) privacy. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, whilst others are qualified, meaning that it is permissible for the state to interfere with the right provided that the interference is in pursuit of a legitimate aim and the interference is proportionate. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR[3]. The use of BWV is 'an interference' and must always be justifiable, therefore the actions of the Trust must be justifiable, have a legitimate aim and the use of video / audio must be proportionate to achieving this. NIAS will carry out a full Data Protection Privacy Impact Assessment in order to address any issues raised by this Article and introduces safeguards associated with how the Trust deploys this equipment in both private and public arenas.

- Freedom of Information Act 2000 – grants a general right of access to all types of recorded information held by public authorities, which will include

[3] Article 8 of the European Charter on Human Rights reads as follows:

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

digital images such as those recorded by body worn video. However in most cases this will be personally identifiable information and exemptions would be used e.g Section 40 – Personal Information and then the request would be placed under a SAR. Procedures are in place to manage subject access requests in respect of video and audio captured using BWV equipment. Each request will be accessed case by case.

- Requests will be managed by NIAS Information Governance Team and will require requesters to provide date, time, and location of the recording together with a suitable means of identification.

- Regulation of Investigatory Powers Act - NIAS is authorised under Section 22(2)(g) – in an emergency preventing death/injury. However, the provisions of RIPA are not applicable to the use of BWV devices, provided it is used overtly in the manner described in this guidance.

- Home Office – Safeguarding Body Worn Video Data (Published October 2018): Supporting Guidance Document and not specific to Northern Ireland

- Information Commissioners CCTV Code of Practice

- Information Commissioner Guidance – Body Worn Video

Policy, Procedures & Training:

If agreed, the implementation of BWV will require the development of a suite of policy and procedural documents along with a training programme to ensure the equipment is used appropriately and within the statutory requirements and guidance, in particular the following will be developed:

- Body Worn Video (BWV) Policy.
- Body Worn Video (BWV) Procedures.
- Body Worn Video (BWV) Standard Operating Procedure.
- Training programme for all designated users and applicable line management.

Training and documentation will include information on the following:

- Key principles.
- Equipment overview.
- Issue / returns / loss.
- Encryption processes
- Recording an incident / starting and ending a recording.
- Consent to use Body Worn Video (BWV).
- Objections to recording.
- Limitations / specific incidents.
- Post incident procedure.
- Viewing and producing evidential copies of footage.
- Data retrieval and management.

- Security of footage and its accessibility to respond to a subject access request.
- Responsibilities.
- Applicable legislation (including function creep).
- Health and safety.

Does the processing actually achieve your purpose as set out in Step 1?

Yes. The operational use of BWV is proportionate, legitimate and necessary; it will be only used when deemed necessary for the purposes of violence reduction, by trained staff in accordance with policy, procedures and legislation.

Is there another way to achieve the same outcome?

No.

NIAS has duty to protect frontline ambulance staff. BWV device implementation is vital to support this and is invaluable as evidence to increase guilty pleas and to supporting:

- Staff, patients and third parties;
- Apprehend and prosecute offenders and provide evidence to take criminal or civil action in the Courts;
- Provide a deterrent effect and reduce unlawful activity;
- Help provide a safer environment for our staff.

How will you prevent function creep (e.g. use of the new system or process in ways beyond the original purpose, that could lead to additional privacy risks)?

NIAS will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. At all stages it will comply with the UK GDPR and Data Protection Act and other legislation such as Human Rights legislation, there will be adherence to the requirements of Article 6 (Right to a fair trial) & in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured & processed to achieve a legitimate aim as detailed.

Policy, Procedures & Training:

If agreed, the implementation of BWV will require the development of a suite of policy and procedural documents along with a training programme to ensure the equipment is used appropriately and within the statutory requirements and guidance, in particular the following will be developed:

- Body Worn Video (BWV) Policy.
- Body Worn Video (BWV) Procedures.
- Body Worn Video (BWV) Standard Operating Procedure.
- Training programme for all designated users and applicable line management.

Training and documentation will include information on the following:

- Key principles.
- Equipment overview.
- Issue / returns / loss.
- Encryption processes
- Recording an incident / starting and ending a recording.
- Consent to use Body Worn Video (BWV).
- Objections to recording.
- Limitations / specific incidents.
- Post incident procedure.
- Viewing and producing evidential copies of footage.
- Data retrieval and management.
- Security of footage and its accessibility to respond to a subject access request.
- Responsibilities.
- Applicable legislation (including function creep).
- Health and safety.

How will you ensure data quality and data minimisation (collection, use and processing the minimum amount of personal to achieve the intended purpose)?

When capturing information on these devices, ambulance staff will only do so in order to fulfil the legitimate purpose, which is to reduce violence and aggression towards staff. Data will only be accessed and stored when a member of staff completes an incident report form via DATIX and advised that footage is available. Footage will then be accessed by one of the five authorised and nominated Trust staff, and stored as it is deemed as evidential. Footage could then be shared with PSNI, Crown Prosecution Service, Defence professionals and the Courts to support a prosecution.

If agreed, the implementation of BWV will require the development of a suite of policy and procedural documents along with a training programme to ensure the equipment is used appropriately and within the statutory requirements and guidance, in particular the following will be developed:

- Body Worn Video (BWV) Policy.
- Body Worn Video (BWV) Procedures.
- Body Worn Video (BWV) Standard Operating Procedure.
- Training programme for all designated users and applicable line management.
- Protocols will also be developed to ensure that no appropriate use of the BWV is being used. For example, cross-referencing system of DATIX

reports and transferred files from BWV devices will be undertaken on a regular basis to ensure no inappropriate use.

What information will you give individuals about this new system / process and how will you support their data protection rights? Have you considered the need for a privacy notice to outline and inform this new processing?

- A separate privacy notice for use of CCTV in ambulance, stations and use of the BWV will implemented and to support other privacy notices already in place for both staff and members of the public.
- A Full Public Consultation will be carried out.
- Social Media Awareness.
- Policies and procedures will be developed to support BWV implementations.
- Robust training plan will be developed to support any BWV implementation.
- The NIAS website will be updated to give members the public information on the use of BWV devices by NIAS staff and outline what rights data subjects have. Information on how to make a SAR for BWV will also be available. Published point of contact for information, complaints and concerns.
- Information Governance and Equality expertise sought on an ongoing basis.
- Staff and Trade Union Engagement process.
- NIAS information asset registers and dataflows will updated.
- Asset tagging for BWV devices will also occur.
- Full training programme for all operators.
- Resources for information security under review.
- Required signage erected / on devices. Overt only.
- Existing Information Governance Processes deemed fit for purpose with regards to information sharing / redaction etc.
- Equipment to be installed and maintained in accordance with manufactures instructions.
- ICT resource and expertise as part of project team.

Will you use any 3rd party to process personal data and what measures will you take to ensure processors comply with their data protection responsibilities?

At this time, it is not known but depending on supplier, devices will be docked and data automatically downloaded to central NIAS server that will be held on site. Any third party will also have a requirement to be registered with the Information Commissioner and any contract arrangements will contain the necessary data protection clauses and requirement.

Will any data be held or processed outside the HSC (NI) network and if so where? How will you safeguard any international transfers?

At this time, it is not known but depending on supplier, devices will be docked and data automatically downloaded to central NIAS server that will be held on site. Any third party will also have a requirement to be registered with the Information Commissioner and any contract arrangements will contain the necessary data protection clauses and requirement.

Step 5: Identify, Assess and Mitigate any data protection risks

In this section you are asked to first identify and describe the specific risks associated with this project/process and assess the nature of potential impact on individuals. You will then describe the measures you could take to reduce each identified risk.

To assist you in identifying potential or likely privacy risks you will find a non-exhaustive list of possible risks at Appendix 3

The HSC Regional Risk Matrix and Regional Impact Table at Appendix 4 will also help you to assess the level of risk.

Identify and Assess Risks				**Mitigate Risks**		
Describe below any specific data protection risks and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary *(See Appendix 3 for examples).*	**Likelihood of harm** 1.Rare 2.Unlikely 3.Possible 4.Likely 5.Almost Certain	**Severity of harm** 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic	**Overall risk** 1.Low 2.Medium 3.High 4.Extreme	**List the various controls that have been or will be put in place to mitigate the risk prior to commencement**	**Effect on risk** Reduced Accepted	**Residual risk** Low Medium High
	Refer to HSC Risk Matrix at Appendix 4 **ENTER NUMBERS BELOW**					
If the purpose of Body Worn Video is not clear to the public, there is a risk that it may be seen as an unjustified intrusion on privacy. The public may feel that they have not consented to the use of the technology. There may be public	**3**	**3**	**Med**	Full public consultation to be carried out as per section on consultation. Information Governance and Equality expertise sought on an ongoing basis.	**Reduced**	**Low**

distrust. Vulnerable groups may be disproportionately impacted.				Privacy notice will be updated for Public, Children and separate one for CCTV. BWV assets added to NIAS information asset register. Legal basis for processing is clear has been identified under Article 6, Article 9 and pursuant to Article 10 of the UK GDPR • Footage provided to PSNI, Police Ombudsman, Health and Safety Executive or other statutory agencies for criminal investigation; Trust copy securely destroyed after 2 years. • Footage required for internal/external employee related investigations, Health and Care Professional Council (HCPC), personal injury claims (and identified as secondary processing); securely destroyed after one year.		

				• Unmarked footage; securely destroyed after 31 days. • Recorded material is Trust information and can be accessed on request in writing in accordance with the data protection legislation unless an exemption applies in the circumstances (Subject Access). The BWV operator will consider on a case-by-case basis whether or not to switch the BWV on or off. There should always be a presumption to record if the operation guidance has been met unless the circumstances dictate otherwise. A member of staff failing to record an incident may be required to justify the actions as vigorously as any member of staff who chooses to record a like encounter. In all cases, recording can only be justified		

				when it is relevant to the incident and necessary in order to gather evidence.		
If the purpose of Body Worn Video is not clear to staff there is a risk that it may be seen as an unjustified intrusion on privacy, wellbeing may be impacted, there may be distrust and relationships with management may be impacted.	**3**	**3**	**Med**	Purpose will be made clear during staff consultation, associated training programmes and as part of the associated policies and procedures. Trade Union colleagues have been engaged with the project from the beginning and sit on the Project Team. An expression of interest for staff to join the Project Team was circulated during July 2020. The project will not progress without due consultation.	**Reduced**	**Low**
Compliance related risks, i.e. failure to adhere to data protection legislation, potential fines from the Information Commissioner for incorrect processing or breaches, privacy requirements, human	**3**	**4**	**High**	BWV is a relatively new technology being deployed by NIAS. However the Trust recognise the concerns regarding privacy issues. Accordingly, this technology	**Accepted**	**Med**

rights legislation and / or sector specific legislation or standards. This may leave the Trust open to the risk of fines, reputational risk, project failure etc.				will only be deployed in an overt manner, using trained staff and in defined operational circumstances. All captured data will be processed to ensure total compliance with the Data Protection and Human Rights legislation, and retained and subsequently disposed of in accordance with the relevant policies and procedures. • NIAS CCTV Policy will be reviewed. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced. • A published point of contact for information, complaints and concerns. • The required CCTV signage on all devices and vehicles. • Training for staff in order that they can confidently		

				engage with members of the public on the matter.		
There is a risk that staff will use the device in circumstances which are not appropriate, continuously, or not within the defined operational requirements.	**3**	**4**	**High**	NIAS will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. At all stages it will comply with the Data Protection Act and other legislation such as Human Rights legislation, there will be adherence to the requirements of Article 6 (Right to a fair trial) & in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured & processed to achieve a legitimate aim as detailed. • NIAS CCTV Policy will be reviewed. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced.	**Accepted**	**Med**

				• A published point of contact for information, complaints and concerns. • The required CCTV signage on all devices and vehicles. • Training for staff in order that they can confidently engage with members of the public on the matter.		
There is a risk that over a period of time project creep will occur, requests could be made to use the data for other purposes.	**3**	**3**	**Med**	NIAS will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. At all stages it will comply with the Data Protection Act and other legislation such as Human Rights legislation, there will be adherence to the requirements of Article 6 (Right to a fair trial) & in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured & processed	**Reduced**	**Low**

				to achieve a legitimate aim as detailed. A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced.		
There is a risk that inappropriate or excessive data will be held, for example: • Audio – this technology allows the capture of both video and audio data which differs from CCTV. As a result persons may feel that they have not consented to the use of the technology. In some instances, the camera itself may not be pointing in the direction of the main incident but that the surrounding audio will still be captured. • Collateral intrusion – in this context extends to the capturing of the movements and actions of other persons	**3**	**3**	**Med**	Audio recording - as previously stated BWV is a new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. In order to ensure that all aspects of an incident are captured, this requires the essential inclusion of audio information in order for this to be complementary to the video data. The other important aspect of the addition of audio information is that in some instances, the camera itself may not be pointing in the direction of the main incident but that the audio will still be captured. This has a significant advantage of protecting all parties to ensure that the actions of the ambulance	**Reduced**	**Low**

when this equipment is being used. It is inevitable that in some circumstances this will occur. • <u>Increase in the quantity of data</u> – BWV is a relatively new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. Accordingly, there will be more data potentially being captured. • <u>Inability to switch off recording</u> – there is a risk that a member of staff may not be able to switch off the recording due to an incident or clinical needs.				service were totally in accordance with the law. Equally, in some instances, the presence of only video evidence without the added context that audio, can fail to adequately provide the full context, for all parties, of an incident or interaction. <u>Collateral intrusion</u> in this context extends to the capturing of the movements and actions of other persons when this equipment is being used. It is inevitable that in some circumstances this will occur, albeit staff are trained to ensure that wherever possible, the focus of their activity is on the aggressor. In circumstances where individuals are captured in any video or audio information and they are unrelated to any offence under investigation, their identities will be protected and anonymised especially should the matter be presented to a court.		

				<u>Increase in the quantity of data</u> – BWV is a relatively new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. Accordingly, there will be more data potentially being captured but the appropriate safeguards, by adherence to legislation and guidance, will ensure that only information that passes a strict test, of being required for a legitimate purpose, can be retained. <u>Inability to switch off recording</u> – staff will be advised to make every effort to ensure devices are switched of when not required. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced. • Training for staff in order that they can confidently		

				engage with members of the public on the matter.		
• There is a risk that a member of staff will fail to dock the device. • There is a risk that the device will not automatically download. • There is a risk that the data will not be marked evidential and be automatically deleted. • In the event that a system is purchased that incorporates the ability to wipe the device remotely, there is a risk that evidential data could be accidently erased.	**3**	**3**	**Med**	Equipment will be installed and maintained as per manufacturer's instructions. Any device issues / failures / incidents will reported via DATIX and investigated. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced. • Training for staff in order that they can confidently engage with members of the public on the matter. Following an activation the member of staff will be returned to the station, follow a 'check-in' process and 'dock' it into a dedicated port that automatically downloads all the captured information onto the server. This information	**Reduced**	**Low**

				cannot be deleted or altered and is encrypted. The member of staff will then complete a DATIX which will flag up that data needed to be retained. One of the five Trust trained and authorised officers will then identify the elements of captured data to be retained via the software and 'mark' the section appropriately. It will then be backed up on to the primary back-up and then secondary back-up if required. Once completed, the contents on the device are deleted and retained as stated. All other material will be automatically erased after 31 days. Training for authorised officers will include information on the remote wipe function and risks if appropriate.		
There is risk that data will be held for inappropriate length of time.	**3**	**3**	**Med**	Any information captured on a device, which is deemed to be	**Reduced**	**Low**

				non-evidential will be automatically deleted after 31 days. The only rationale for any retention beyond an immediate disposal include circumstances where staff have been subject to violence and aggression in the course of their duties, and there is a desire to review the incident as part of a police investigation. In these circumstances, NIAS Information Governance Team will retain a master copy and it will be stored in line with the Trusts Retention Scheme. Data within the evidential category which has been passed to PSNI, courts etc. will be reviewed and disposed of, in accordance with timeframes within the justice system.		
• <u>Recording in private dwellings</u> – If the purpose of Body Worn Video is not clear to the public,	**3**	**3**	**Med**	<u>Recording in private dwellings</u> – It is widely recognised that citizens are likely to have a strong expectation of privacy	**Reduced**	**Low**

there is a risk that it may be seen as an unjustified intrusion on privacy. • <u>State of undress</u> – there is a risk that footage may show persons in a state of undress. • <u>Access requests</u> – there is a risk that there will be an increase in requests for data and the Trust will not be able to process the requests in a timely way.				especially in their own homes. Indeed this is contained with Article 8 of the ECHR (a right to respect for a private and family life) and under normal circumstances BWV would not be used in private dwellings. However if the user is present at an incident in a private dwelling, and there is a risk of violence and aggression, then there is a genuine purpose and this equipment is able to be used. The user will be mindful to exercise discretion and recording should only be used when it is relevant to the incident and necessary in order to gather evidence, all recordings require a lawful basis in order to justify infringement of Article 8. In circumstances where an occupant of the premises objects to the recording taking place but where an incident is taking place staff are recommended to continue with		

				a recording but explain their reasons for doing so. These reasons might include: • That an incident has occurred requiring police to attend. • That the member of staffs continued presence might be required to provide emergency care. • There is a requirement to secure best evidence of any offences that have occurred and that the video/audio evidence will be more accurate and of a higher quality and therefore in the interests of all parties. • That continuing to record would safeguard both parties, with a true and accurate recording of any significant statement made by either party and of the scene		

				• That the incident may reoccur in the immediate future • That continuing to record will safeguard the BWV user against any potential allegations from either party. NIAS is very mindful of the concerns that this raises and will train its users to respect and adhere to these safeguards. When capturing information on these devices, ambulance staff will only do so in order to fulfil the legitimate purpose, which is to reduce violence and aggression towards staff. Data will only be accessed and stored when a member of staff completes an incident report form via DATIX and advised that footage is available. Footage will then be accessed by one of the five authorised and nominated Trust staff, and		

				stored as it is deemed as evidential. Footage could then be shared with PSNI, Crown Prosecution Service, Defence professionals and the Courts to support a prosecution. Any captured information deemed to be evidential, will in the first instance be 'protected' by means of a Master copy being created. This remains an integral part of the process. A Working copy(s) is created and it is this which will be passed to PSNI. In instances of any dispute, the Court can require the production of the Master copy. Other various access requests will be dealt with via existing information governance arrangements, i.e. via the Information Governance Team. NIAS will review resources required longer term for the management of security related matters.		

• It is also possible that in some circumstances, such as within a public order or violent encounter, a device might become detached from a member of staff and fall into the hands of unauthorised persons. This presents the possibility of the data being accessed by an unauthorised individual. • There is a risk that a device or RFID will be lost or stolen. • There is a risk of unauthorised access to and / or unauthorised copying of data. • There is a risk of claims for compensation as a result of data loss. • There is a risk of a cyber-security incident / data being accessed by unauthorised persons.	**3**	**4**	**High**	This technology will only be deployed in an overt manner, using trained staff and in defined operational circumstances. All captured data will be processed to ensure total compliance with the Data Protection and Human Rights legislation, and retained and subsequently disposed of in accordance with Trust Policy. Due to the very nature of pre hospital care, it is possible that in some circumstances, such as within a public order or violent encounter, a device might become detached from a member of staff and fall into the hands of persons and therefore potentially lost with the possibility of the data being accessed by an unauthorised individual. The means of attaching equipment to the uniform has been subject of	**Accepted**	**Med**

• There is a risk of data loss due to human error, failure to back up server, viruses, network failure, fire, flood etc.				much consideration and is designed to physically reduce instances of the equipment being ripped from a member of staff. Attachments to uniforms will be tested as part of implementation. Devices will likely have RFID and booked out to an individual from a pool of devices. As such, the impact in terms of any time lost between any actual loss and notification to the Trust, is kept to a minimum. Where a device is lost, it will be reported immediately to the Information Governance Team and or the most senior officer on call. The device is encrypted and there is a limited amount of captured information stored on the device's internal memory and requires specific docking facilities to access the footage. In the event of a loss the Trust		

				intends to have the ability to locate via GPS and remote wipe. In terms of cyber security, a device is docked in order to transfer data, therefore the entire Trust network would have to be hacked for it to be at risk. Also the device is encrypted and there is a limited amount of captured information stored on the device's internal memory and requires specific docking facilities to access the footage. In addition it is important to note that the recording itself is encrypted, as it records, not the device. AES256 standard. Only the software can decrypt it, so when it is uploaded to Trust storage systems, the recording remains encrypted. Depending on supplier, it is likely that the software decrypts the recording and		

				stores separately, therefore two versions exist, an encrypted and a decrypted. The software may also be able to auto purge all decrypted recordings. The procedures and principles applicable to BWV are similar to how the Trust handles requests or court orders for CCTV data. Issues relating to these requests will be referred to the Information Governance Team and escalated through senior management as necessary. Depending on supplier, devices are likely to be docked and data automatically downloaded to central server and is not accessible by staff or line management locally. Footage will only be accessed by one of the five authorised and nominated Trust staff via PCs with personal logins, and		

				only held past 31 days if it is deemed as evidential. The Trust has an ICT resource and expertise as part of project team. Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged, i.e. footage will be supplied for evidential purposes only. It will be decrypted using the software and emailed to IT requesting it to be put on a password protected DVD/CD. Footage must be requested by authorised police staff and collected by hand under signature. Immediate supply for life/death, detection of crime incidents will be provided in written request of a police officer of at least Inspector rank. In all cases a Form 81 will be required. Master copy will be retained securely on-		

				site with the Information Governance Team. Trust Business Continuity Policies, Procedures and Plans are in place. Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged.		

Step 6. SIGN OFF and record outcomes

a. Project Lead / Service Lead

The Project / Service Lead sign-off confirming they have or will:

- *review any consultation responses, provide any required explanation on outcome and explain reasons if decision departs from the views of any stakeholders.*
- *accept and approve any measures outlined in the DPIA and integrate actions back into the project plan*
- *ensure appropriate data sharing arrangements are put in place where data is shared with third party organisations (e.g.: Contracts, Data Access Agreements, Data Sharing Agreements)*
- *consider the need for a Privacy Notice to inform service users of how their personal data is to be processed; and if appropriate put this in place*
- *keep the DPIA under review*

Project /Service Lead Comments:

- Ongoing monitoring of consultation.
- Mitigations accepted and will be implemented.
- Any necessary additional data sharing agreements will be put in place.
- Privacy notice will be updated.
- DPIA will be kept under review.

Name: Katrina Keating

Job Title: Risk Manager

Signed: 	**Date: 24/08/2021**

b. Data Protection Officer (DPO)

The DPO should:

- *Advise on compliance, 'step 5' mitigating measures and whether processing can proceed.*
- *Ensure the DPIA is added to central DPIA Register (by Information Governance)*

Summary of DPO advice:

The detailed background, risk descriptions and mitigating measures (to reduce or eliminate risks) in this DPIA indicate that there are appropriate technical and organisational measures in place for NIAS to lawfully utilise BWV devices as described. The DPIA is sufficient to implement the data protection principles effectively and safeguard individual rights in this case.

Name: Tracy Avery

Signed:	**Date**: 23/11/2021

c. Information Asset Owner (IAO)

The IAO should:

- *Consider and approve any residual risks. If accepting any residual high risk, you should consult the Information Commissioner's Office (ICO) before going ahead.*
- *Ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training*
- *Make arrangements for any new systems to be added to the Information Asset Register (IAR) or update an existing entry to reflect new processing*

IAO Comments:

Name: Pending

Title: Pending

Signed:	**Date**:

Please return signed DPIA to Information Governance Department

Appendix 1 - Data Protection Principles

The data protection principles are contained in the UK GDPR and require that personal information must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject - (Lawfulness, Fairness and transparency). There must be valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data and you must not do anything with the data in breach of any other laws. Personal data must be processed in a way that is fair and not unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (Purpose limitation)

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Storage Limitation)

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

In accordance with Article 5(2) of the UK GDPR the data controller shall be responsible for, and through its policies, procedures and protocols will demonstrate compliance with the Data Protection Principles listed above **(overarching principle of Accountability).**

Appendix 2 – Lawful Basis for processing Personal Information and Special Category Information

You must have a valid lawful basis in order to process personal data in compliance with Article 6 of UK GDPR.

If you are processing special category data*, you also need to identify a further special category condition in compliance with Article 9 of UK GDPR.

You should document your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability

The lawful bases for processing are set out in **Article 6 of the UK GDPR**. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. *(NB. Please consult with your IG Department before using this as your lawful basis for processing personal data. This cannot be applied by a public authority processing data to perform its official / core function (e.g. processing data as part of the provision of health or social care) however may be relevant for non-core functions such as HR)*

Special category data is personal data that needs more protection as it is more sensitive than basic personal data. The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Article 9 lists the conditions for processing special category data:

(a) Explicit consent

(b) Employment, social security and social protection (if authorised by law)

(c) Vital interests

(d) Not-for-profit bodies

(e) Made public by the data subject

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

(j) Archiving, research and statistics (with a basis in law)

See the Information Commissioner's Office (ICO) website (links below):

- For more detail on each lawful basis for processing personal data

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

- For more detail on the additional conditions for processing special category (sensitive) personal data

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Appendix 3 - Examples of possible risks include:

Risks to individuals
• Inadequate disclosure controls increase the likelihood of information being shared inappropriately. • The context in which the information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. • New surveillance methods may be an unjustified intrusion on their privacy. • Measures taken against individuals as a result of collecting information about them might be seen as intrusive. • The sharing and merging of datasets can allow organisations to collect a much wider range of information than individuals might expect. • Identifiers might be collected and linked, which prevent people from using a service anonymously. • Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. • Collecting information and linking identifiers might mean that the organisation is no longer using information that is safely anonymised. • Information that is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk. • If a retention period is not adhered to in line with the DoH retention and disposal guidelines as set out in the document Good Management Good Records (GMGR), information might be used for longer than necessary. • The use of biometric information or potentially intrusive tracking technologies may cause increased concern.

Whilst a DPIA is concerned with the risks to individuals, there may be other types of risk that are linked with the processing which services should consider.

Corporate or Compliance risks

• Non-compliance with data protection and other legislation can lead to enforcement action, fines and reputational damage, for example:
  • Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
  • Non-compliance with Human Rights legislation.
  • Non-compliance with sector specific legislation or standards.
• Problems that are only identified after the project has launched are more likely to require expensive fixes.
• Information that is collected and stored unnecessarily or is not properly managed so that duplicate records are created is less useful to service areas.
• Public distrust about how information is used can damage the organisation's reputation.
• Data losses that cause damage or distress to individuals could lead to claims for compensation against the organisation.

Appendix 4 – HSC Regional Impact Table and HSC Regional Risk Matrix
– With effect from April 2013 (updated June 2016 & August 2018)

HSC REGIONAL RISK MATRIX

Risk Likelihood Scoring Table			
Likelihood Scoring Descriptors	**Score**	**Frequency (How often might it/does it happen?)**	**Time framed Descriptions of Frequency**
Almost certain	5	Will undoubtedly happen/recur on a frequent basis	Expected to occur at least daily
Likely	4	Will probably happen/recur, but it is not a persisting issue/circumstances	Expected to occur at least weekly
Possible	3	Might happen or recur occasionally	Expected to occur at least monthly
Unlikely	2	Do not expect it to happen/recur but it may do so	Expected to occur at least annually
Rare	1	This will probably never happen/recur	Not expected to occur for years

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant(1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely (4)	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible (3)	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely (2)	**Low**	**Low**	**Medium**	**High**	**High**
Rare (1)	**Low**	**Low**	**Medium**	**High**	**High**

HSC Regional Impact Table

DOMAIN	IMPACT (CONSEQUENCE) LEVELS [can be used for both actual and potential]				
	INSIGNIFICANT (1)	**MINOR (2)**	**MODERATE (3)**	**MAJOR (4)**	**CATASTROPHIC (5)**
PEOPLE *(Impact on the Health/Safety/Welf are of any person affected: e.g. Patient/Service User, Staff, Visitor, Contractor)*	• Near miss, no injury or harm.	• Short-term injury/minor harm requiring first aid/medical treatment. • Any patient safety incident that required extra observation or minor treatment e.g. first aid • Non-permanent harm lasting less than one month • Admission to hospital for observation or extended stay (1-4 days duration) • Emotional distress (recovery expected within days or weeks).	• Semi-permanent harm/disability (physical/emotional injuries/trauma) (Recovery expected within one year). • Admission/readmission to hospital or extended length of hospital stay/care provision (5-14 days). • Any patient safety incident that resulted in a moderate increase in treatment e.g. surgery required	• Long-term permanent harm/disability (physical/emotional injuries/trauma). • Increase in length of hospital stay/care provision by >14 days.	• Permanent harm/disability (physical/ emotional trauma) to more than one person. • Incident leading to death.
QUALITY & PROFESSIONAL STANDARDS/ GUIDELINES *(Meeting quality/ professional standards/ statutory functions/ responsibilities and Audit Inspections)*	• Minor non-compliance with internal standards, professional standards, policy or protocol. • Audit / Inspection – small number of recommendations which focus on minor quality improvements issues.	• Single failure to meet internal professional standard or follow protocol. • Audit/Inspection – recommendations can be addressed by low level management action.	• Repeated failure to meet internal professional standards or follow protocols. • Audit / Inspection – challenging recommendations that can be addressed by action plan.	• Repeated failure to meet regional/ national standards. • Repeated failure to meet professional standards or failure to meet statutory functions/ responsibilities. • Audit / Inspection – Critical Report.	• Gross failure to meet external/national standards. • Gross failure to meet professional standards or statutory functions/ responsibilities. • Audit / Inspection – Severely Critical Report.

REPUTATION *(Adverse publicity, enquiries from public representatives/media Legal/Statutory Requirements)*	• Local public/political concern. • Local press < 1day coverage. • Informal contact / Potential intervention by Enforcing Authority (e.g. HSENI/NIFRS).	• Local public/political concern. • Extended local press < 7 day coverage with minor effect on public confidence. • Advisory letter from enforcing authority/increased inspection by regulatory authority.	• Regional public/political concern. • Regional/National press < 3 days coverage. Significant effect on public confidence. • Improvement notice/failure to comply notice.	• MLA concern (Questions in Assembly). • Regional / National Media interest >3 days < 7days. Public confidence in the organisation undermined. • Criminal Prosecution. • Prohibition Notice. • Executive Officer dismissed. • External Investigation or Independent Review (e.g., Ombudsman). • Major Public Enquiry.	• Full Public Enquiry/Critical PAC Hearing. • Regional and National adverse media publicity > 7 days. • Criminal prosecution – Corporate Manslaughter Act. • Executive Officer fined or imprisoned. • Judicial Review/Public Enquiry.
FINANCE, INFORMATION & ASSETS *(Protect assets of the organisation and avoid loss)*	• Commissioning costs (£) <1m. • Loss of assets due to damage to premises/property. • Loss – £1K to £10K. • Minor loss of non-personal information.	• Commissioning costs (£) 1m – 2m. • Loss of assets due to minor damage to premises/ property. • Loss – £10K to £100K. • Loss of information. • Impact to service immediately containable, medium financial loss	• Commissioning costs (£) 2m – 5m. • Loss of assets due to moderate damage to premises/ property. • Loss – £100K to £250K. • Loss of or unauthorised access to sensitive / business critical information • Impact on service contained with assistance, high financial loss	• Commissioning costs (£) 5m – 10m. • Loss of assets due to major damage to premises/property. • Loss – £250K to £2m. • Loss of or corruption of sensitive / business critical information. • Loss of ability to provide services, major financial loss	• Commissioning costs (£) > 10m. • Loss of assets due to severe organisation wide damage to property/premises. • Loss – > £2m. • Permanent loss of or corruption of sensitive/business critical information. • Collapse of service, huge financial loss

RESOURCES *(Service and Business interruption, problems with service provision, including staffing (number and competence), premises and equipment)*	• Loss/ interruption < 8 hour resulting in insignificant damage or loss/impact on service. • No impact on public health social care. • Insignificant unmet need. • Minimal disruption to routine activities of staff and organisation.	• Loss/interruption or access to systems denied 8 – 24 hours resulting in minor damage or loss/ impact on service. • Short term impact on public health social care. • Minor unmet need. • Minor impact on staff, service delivery and organisation, rapidly absorbed.	• Loss/ interruption 1-7 days resulting in moderate damage or loss/impact on service. • Moderate impact on public health and social care. • Moderate unmet need. • Moderate impact on staff, service delivery and organisation absorbed with significant level of intervention. • Access to systems denied and incident expected to last more than 1 day.	• Loss/ interruption 8-31 days resulting in major damage or loss/impact on service. • Major impact on public health and social care. • Major unmet need. • Major impact on staff, service delivery and organisation - absorbed with some formal intervention with other organisations.	• Loss/ interruption >31 days resulting in catastrophic damage or loss/impact on service. • Catastrophic impact on public health and social care. • Catastrophic unmet need. • Catastrophic impact on staff, service delivery and organisation - absorbed with significant formal intervention with other organisations.
ENVIRONMENTAL *(Air, Land, Water, Waste management)*	• Nuisance release.	• On site release contained by organisation.	• Moderate on site release contained by organisation. • Moderate off site release contained by organisation.	• Major release affecting minimal off-site area requiring external assistance (fire brigade, radiation, protection service etc).	• Toxic release affecting off-site with detrimental effect requiring outside assistance.