Check list for handling Personal Information
Before, During and After an Emergency

The most common type of an emergency we would likely have here in The Bahamas is a hurricane.

Before an Emergency

1. Identify legislative authorities.

Understand your legislative authority to disclose and under what conditions. Refer to Section 13 of the Data Protection (Privacy of Personal Information) Act, 2003, (the DPA).

2. Draft a policy and procedures.

This will help staff know what they need to do when confronted with a request for personal information from a government body, non-governmental organization, individuals or the media.

- **Specify the purposes:** If your organization wishes to be in a position to notify an individual's friends and family about their loved ones in emergency or disaster situations, you should include this purpose in your list of purposes for which personal information can be used or disclosed and communicate this fact to your customers/clients through your consent forms and privacy policy. This will provide greater flexibility to disclose personal information to family members and others on compassionate grounds in cases where the narrow conditions for exceptional disclosures cannot be met.

- **Treat sensitive personal information with added care:** Recognize that sensitive personal information, such as health or financial information should be handled with additional precautions (e.g. additional scrutiny with respect to limiting purposes for using the information, ensuring secure storage, etc.).

- Remember the DPA is only concerned with living individuals and persons seeking information about a

deceased individual should be directed elsewhere, (probate jurisdiction etc.**).**

3. Establish a decision-making framework.

Include a decision-making framework on the release of personal information, in line with the organization's broader emergency policy, to cover legislative requirements and to help guide the exercise of discretion in disclosing personal information.

4. Ensure the quality of your information.

Take steps to ensure personal information held by your organization is accurate, complete and up to date – so it will be of maximum assistance during an emergency.

5. Establish information sharing protocols where necessary.

If your organization may be in a position to offer assistance, you could establish information-sharing arrangements with emergency management organizations [(e.g. National Emergency Management Authority) NEMA] to coordinate action within the limits of the applicable legislative authority.

In addition to NEMA, information if requested may also be shared with the Police and Red Cross Society and other relevant agencies, such as the Defense Force and Immigration.

Disclosing organizations should consider the following elements in developing a protocol for data sharing in an emergency:

- **Set start and end dates:** Be clear about the period during which the data sharing arrangements will be in place and set a clear end date.

- **Establish who else will have access:** Define and limit the other organizations with which personal information is to be shared. Ensure that the requesting emergency authority explains its reasons for seeking the information.

- **Set out the decision-making framework:** Based on the authorities for disclosure, establish how the information will be disclosed and who must authorize it.

- **Identify the personal information data elements that need to be shared at each stage of the authorization process:** This will ensure that what is shared is only what is required for the purpose.

- **Restrict disclosures to those purposes which relate *directly* to the emergency:** Clarifying how much information is necessary, and tailoring the disclosure to the actual purpose, helps both the disclosing organization and receiving organization.

- **Request that the information be kept separately from the receiving organization's existing systems.** This will allow it to be securely archived and/or disposed of when no longer needed to respond to, or recover from, the emergency.

- **Ensure the security of the information:** Specify that the personal information must be secure while in transit and kept securely stored once received (e.g. encryption, technical and administrative access controls.)

- **Address destruction/disposal:** Set a regime for destruction/disposal of the personal information once the information is no longer needed, in compliance with legislative obligations.

- **Enable access and correction rights:** Establish procedures for allowing individuals to access and, where necessary, correct their personal information.

- **Identify someone to answer questions and respond to complaints:** Ensure there are policies and procedures to handle complaints and encourage individuals to contact the Data Protection Commissioner in case of need.

6. Train your people how to respect privacy in an emergency situation.

Provide training to the emergency response organization on privacy generally, but also specifically on how to deal with privacy in an emergency situation.

Including personal data sharing scenarios in your broader emergency training plans will help your organization develop a better understanding of the decisions that may need to be made and how to apply the relevant policies and procedures.

7. Consider how you will make the transition from the official end of an emergency to the resumption of normal information handling practices.

Establish procedures to deal with the transition period between the official end to the emergency and the resumption of normal information handling practices. Consider that, when the official emergency period ends, it is unlikely to mean an end to the extraordinary circumstances facing the people, businesses and agencies affected.

During an Emergency

1. Consult your privacy policies and procedures and use the decision making framework.

Follow your policy and procedures and use the decision-making framework established before the emergency to help guide decisions and actions. Identify and locate the individuals in your organization who have the appropriate delegated authority to release personal information in exceptional circumstances.

2. Be responsive and ready to act.

Not all situations can be planned for and you may decide or be asked to share personal information in situations that are not governed by the usual rules and procedures. Remember, it is reasonable to share health information to carry out a statutory function (like being a first responder) or helping the individual when they are not able to give consent.

For example, someone's family or friends may ask you whether their loved one was affected by, or escaped, the incident or perhaps their whereabouts. If your organization has included this purpose in the list of purposes for which personal information can be used, it will provide you with flexibility to respond in such situations.

3. Where there is no information sharing protocol in place, get answers on key information handling questions before disclosing to another organization.

- Ideally, you would have an information sharing protocol in place with the organization requesting information, but this is not going to be possible in all situations. Before disclosing personal information:

- **Ensure the organization explains its reasons for seeking the personal information and its authority to do so.** This will give your organization added confidence about making the disclosure under your decision-making framework.

- **Minimize the disclosure:** Clarify how much personal information is necessary, and tailor the disclosure to the actual purpose to minimize the amount of personal information to be disclosed. Disclosures of personal information should be restricted to those purposes which relate *directly* to the emergency. This should reflect the approach of your information sharing/privacy plan.

- **Limit the purposes of its use:** Ensure that recipients of the information clearly understand that the personal information is being disclosed for limited purposes related to an emergency only.

- **Ensure sensitive personal information will be treated with additional care:** Sensitive personal information, such as health or financial information, should be treated with additional precautions (e.g. additional scrutiny with respect to limiting purposes for using the information and ensuring secure storage).

- **Address security:** Ensure that the personal information will be transmitted and stored securely to protect it from misuse, loss, unauthorized access, modification or disclosure.

4. Make an effort to document any disclosures of personal information.

Where possible, make a record of any disclosures:

- the personal information that was disclosed;
- when it was provided;
- to whom it was given;
- the purposes for which it were disclosed;
- who authorized the transfer;
- the legislative authority under which it was provided; and
- any restrictions on how it is to be handled later, such as how long it is to be retained and whether it is to be returned.

5. Notify individuals of any disclosures.

Where possible, notify individuals, or next of kin, in writing about personal information disclosed, for emergency purposes, prior to or as soon as possible thereafter.

After an Emergency

When the official emergency period ends, this is unlikely to mean an end to the extraordinary circumstances facing the people, businesses and agencies affected. However, it may be difficult to determine the length of time required to keep on following emergency procedures related to data sharing.

1. Consult your privacy policies and procedures on resuming normal information handling practices.

Follow the procedures your organization has established to deal with the transition period between the official end to the emergency and the resumption of normal information handling practices.

Organizations should be aware that they may need to continually be assessing whether an emergency exists.

Normal rules and procedures for collecting, using and disclosing personal information should resume as soon as possible following the end of the emergency, but the date should be one a reasonable person

would expect in the circumstances. Notice about resuming normal rules should be widely publicized.

2. Follow up on the information you disclosed.

Make inquiries to determine whether the information was used correctly, in accordance with the legislative requirements and organizational policies.

3. Evaluate and update your policies and practices as required.

- Review the policies, procedures and training, analyze how effective they were and determine whether there is any scope for improvement.

- Update policies and procedures, protocols, sharing agreements and training with respect to privacy practices as required.

Throughout the whole process always remember that:-

"Privacy is the Best Policy!"

(Adapted-Privacy Commissioner of Canada)