Review of GP IG risks

Leeds CCG IG team carried out a review of DATIX incidents reported as either "IG" or "patient confidentiality" from all practices across the city for the period September 18 to September 19.

After review, 187 IG incidents were sorted into broad categories (under this we have included delays in actioning or filing information as they are information incidents under the "accuracy and integrity" principles of GDPR) and a root cause analysis was carried out to try to identify the most common "IG Risks" for practices.

The breakdown of these result are as follows:

Category/type	Number incidents	Meaning/examples	Risk and/or consequence	Mitigation
confidentiality breach	40	Data provided in confidence but divulged inappropriately.	Potential breach of common law duty of confidentiality, the integrity & confidentiality principle and individuals rights under Data Protection Legislation	Ensure that all staff are aware of the rules regarding confidentiality and that robust and effective procedures are in place in regards to this.
delay in filing/actioning	26	Delays in filing or actioning data received, that have resulted in an adverse consequence for the patient	Adverse consequences for patient care due to a delay in treatment and a breach of Data Protection legislation principles (Accuracy and Integrity of records)	Ensure that procedures are in place to ensure that all incoming data is processed effectively and in a timely manner
filed in incorrect record	19	Data filed into an incorrect record, either by the current practice, or discovered as part of a review of records (by either a member of staff or the patient)	Potential adverse consequences for patient care due to incorrect data being acted upon and a breach of Data Protection legislation principles (Accuracy and Integrity of records)	Ensure that procedures are in place to ensure that data is filed correctly and that there is a clear understanding of when and how amendments to records can be made, and by whom.
Incorrect patient details in document received	13	Information received into the practice that containing incorrect data, that was intercepted before it was added to the record	Potential adverse consequences for the patient if the data had not been intercepted (and potential adverse consequence to an unknown patient for whom the data did apply, regardless of interception).	Ensure robust procedures in place for checking patient details upon receipt of data
delay in receipt of data	11	A delay in receipt of data which has resulted in an adverse consequence for the patient	Adverse consequences for patient care due to a delay in treatment and a breach of Data Protection legislation principles (Accuracy and Integrity of records) on the part of the sender	Very little mitigation available to the practice other than to ensure that "late" data is processed effectively and in a timely manner to minimise the change of an adverse effect upon the patient.
accuracy or quality of data	11	Issues with the accuracy of the data within a record (due to misfiling etc,) where the data is incorrect (so	Potential adverse consequences for patient care due to incorrect data being acted upon, with a possible corresponding effect upon the patient	Difficult to mitigate against, as generally a historical issue, but ensure that procedures are in place and that there is a clear

		possibly misfiled, but it has been unable to identify which record the data should have been)	that the data should have been filed against and a breach of Data Protection legislation principles (Accuracy and Integrity of records)	understanding of when and how amendments to records can be made, and by whom.
Incorrect patient details accessed	10	The incorrect patient details were accessed for the purposes of booking appointment etc, with some potentially adverse consequences	Potential breach of confidentiality if incorrect patient details are accessed.	Ensure that there is a procedure in place for positively checking a patients identity e.g. by cross referencing multiple identifiers name, DoB, Address etc
prescription provided to wrong patient	10	A prescription given to the wrong patient.	Breach of confidentiality as health data released to the wrong individual and potential adverse effect due to delay in correct patient receiving medication	Reinforce the importance of checking repeat scripts before release, especially if repeats are stapled together
Online access granted incorrectly	9	Online access granted to a patient, but due to issues such as substandard ID checks, access to another patient's record provided	Breach of confidentiality as health data released to the wrong individual	Ensure that there is a procedure in place for positively checking a patients identity e.g. by cross referencing multiple identifiers name, DoB, Address etc
data received for non-patient	9	Data received into the practice for a patient who has either never been a patient, is no longer a patient, or is deceased	Breach of confidentiality as health data released to the wrong health professional	Ensure that there is a procedure in place for "returning" the data via the correct mechanism
incorrect recipient	6	Data sent in error to the wrong recipient	Breach of confidentiality as health data released to the wrong individual	Ensure procedures in place to ensure that data is being sent to the correct recipient by checking NHS.Net address, fax number etc before releasing information
"lost" data	5	Data which should have been received and filed, but for which there is no trace due to deletion or loss	Breach of the "Integrity" Principle due to data being "lost" (or possibly misfiled)	Very little mitigation available to the practice other than to ensure that data is processed effectively and in a timely manner to minimise the change of an adverse effect upon the patient.
Issues regarding disclosure/records release	4	Issues regarding the improper disclosure of data, generally via Subject Access	Breach of confidentiality due to the disclosure of data to improper or inappropriate recipients	Ensure procedures are in place to check that any proposed recipient of personal and confidential data has a legitimate reason for access to that information
Physical Access to "confidential" area	3	Issues where an unauthorised person has managed to access parts of the building which should be restricted	A security breach that could have ramifications on a number of data protection issues, including a loss of integrity and confidentiality.	Ensure that physical barriers and security measures are in place to ensure that unauthorised persons cannot access areas where personal data is stored (in either electronic or paper formats)

delay in sending information	3	Delays in sending data, that have resulted in an adverse consequence for the patient	Adverse consequences for patient care due to a delay in treatment and a breach of Data Protection legislation principles (Accuracy and Integrity of records)	Ensure that procedures are in place to ensure that all data that requires transfer is processed effectively and in a timely manner
Incorrect patient details on document sent	2	Data sent from the practice, containing incorrect patient information	Potential adverse consequences for the patient if the data had not been intercepted (and potential adverse consequence to an unknown patient for whom the data did apply, regardless of interception).	Ensure robust procedures in place for checking patient details prior to transfer of data
Theft or loss of hardware/device/script	2	In these two cases; a laptop and a stack of prescriptions	Numerous potential consequences from the loss including breaches of confidentiality, potential fraud and reputational damage	Ensure that physical barriers and security measures are in place to ensure that unauthorised persons cannot access “staff only” areas.
use of unsecure transfer method	1	i.e. unsecure email	Possible breach of confidentiality if data is intercepted due to a lack of security protocols in the method used	Ensure procedures in place to ensure that data is being sent by an appropriate transfer method before releasing information
insufficient patient data shared	1	Data sharing where the data shared was not enough for the required purpose	Potential adverse consequences for patient care due to insufficient data being acted upon, and a breach of Data Protection legislation principles (Accuracy, Integrity of records and data minimisation)	Ensure that when data is shared all relevant is included
Spam/Phishing email	1	Note- since compiling this report there have been several more reports of phishing emails	Numerous potential adverse consequences, depending on the nature of the email	Ensure that all staff are aware of the characteristics of a “spam” email